FORTINET
High Performance Network Security

FortiClient - Administration Guide

VERSION 5.4.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

May 12, 2017

FortiClient 5.4.3 Administration Guide

04-543-292132-20170512

TABLE OF CONTENTS

Change Log **8**
Introduction **9**
FortiClient modes and features 9
Standalone mode 11
Managed mode 11
Fortinet product support for FortiClient 11
FortiClient EMS 12
FortiManager 12
FortiGate 13
FortiAnalyzer 13
FortiSandbox 13
Licensing 14
FortiClient licenses for FortiGate 14
FortiClient licenses for EMS 14
Installation requirements 14
Firmware images and tools 15
Microsoft Windows 15
Mac OS X 16
What's New in FortiClient 5.4 ..... **18**
FortiClient 5.4.3 18
FortiClient 5.4.2 18
FortiClient 5.4.1 18
Endpoint control 18
Vulnerability scan 19
FortiSandbox support for removable media 20
Configurator tool 20
FortiClient 5.4.0 20
Antivirus 20
Web Filtering 21
VPN 21
Endpoint Control 22
FortiClient GUI 24
Logging 24
Standalone FortiClient **25**

About standalone mode 25
Get started 25
Provision and configure 25
Use FortiClient console 25
Managed FortiClient 26
About managed mode 26
FortiClient profiles 26
FortiClient Telemetry connection options 28
Telemetry Gateway IP Lists 31
On-net / off-net status with FortiGate and EMS 31
Get started 32
Configure endpoint management 32
Provision FortiClient 33
Use FortiClient console 33
Configure FortiGate 34
Get started 34
Enable the Endpoint Control feature 34
Enable FortiTelemetry on an interface 34
Configure firewall policies 35
Configure FortiClient profiles 36
Enable a key password for FortiTelemetry connection 37
Monitor FortiClient endpoints 38
Configure FortiClient Telemetry connections with AD user groups 38
Configure users and groups on AD servers 38
Configure FortiAuthenticator 38
Configure FortiGate or EMS 38
Connect FortiClient Telemetry to FortiGate or EMS 40
Monitor FortiClient connections 40
FortiClient Provisioning 42
Download FortiClient installation files 42
Install FortiClient on computers 42
Microsoft Windows computer 42
Microsoft Server 44
Mac OS X computer 45
Install FortiClient on infected systems 45
Install FortiClient as part of cloned disk images 46
Deploy FortiClient using Microsoft Active Directory servers 46
Deploy FortiClient using EMS 47
Upgrade FortiClient 48
FortiClient Telemetry Connection 49
How FortiClient locates FortiGate or EMS 49
Connect FortiClient Telemetry after installation 50

Remember gateway IP addresses 50
Compliance **52**
Enable compliance 52
Connect FortiClient Telemetry manually 52
Disconnect FortiClient Telemetry 53
View compliance status 53
Standalone mode 53
FortiClient Telemetry connected to EMS 54
FortiClient Telemetry connected to FortiGate 55
View user details 56
View gateway IP lists 57
Forget gateway IP addresses 58
Fix not compliant status 58
View not-compliant status 58
View compliance rules 59
Fix now 60
Manually fix software vulnerabilities 61
Examples of blocked FortiClient endpoints 61
View notifications 62
Antivirus **63**
Enable/disable realtime protection 63
Enable/disable Antivirus 63
Enable/disable FortiSandbox 64
Block access and communication channels 65
Enable/disable FortiSandbox scanning of files on removable media 65
Scan and analysis on demand 65
Scan now 65
Scan files or folders 66
Submit files for analysis 66
Scan with FortiSandbox on demand 66
View FortiClient engine and signature versions 66
Schedule antivirus scanning 67
Add files or folders to exclusion lists 68
View scan results 69
View quarantined threats 69
View site violations 70
View alerts 71
View realtime protection events 72
Configure Antivirus logging 72
Configure Antivirus options 73
Web Security/Web Filter **74**
Enable/disable Web Security/Web Filter 74

Enable/disable Web Security 74
Enable/disable Web Filter 75
Configure Web Security profiles 75
Edit Web Security exclusion lists 76
Configure Web Security settings 78
View violations 78
Application Firewall 80
Enable/disable Application Firewall 80
View application firewall profiles 80
View blocked applications 81
IPsec VPN and SSL VPN 82
Add new connections 82
Create SSL VPN connections 82
Create IPsec VPN connections 83
Connect to VPNs 86
Access to certificates in Windows Certificates Stores 86
Save password, auto connect, and always up 88
Advanced features (Microsoft Windows) 88
Activate VPN before Windows Log on 89
Connect VPNs before logging on (AD environments) 89
Create redundant IPsec VPNs 89
Create priority-based SSL VPN connections 90
Advanced features (Mac OS X) 90
Create redundant IPsec VPNs 91
Create priority-based SSL VPN connections 91
VPN tunnel & script 92
Windows 92
OS X 93
Vulnerability Scan 94
Enable vulnerability scan 94
Enable vulnerability scan in FortiClient profiles (EMS) 94
Enable vulnerability scan in FortiClient profiles (FortiGate) 94
Scan now 95
View scan results 95
View details of scan results 98
Install remediation patches 99
Settings 101
Backup or restore full configuration 101
Signature updates 101
Logging 101
Sending logs to FortiAnalyzer or FortiManager 103
VPN options 104

Certificate management 104
Antivirus options 104
Advanced options 105
Single Sign-On mobility agent 106
FortiClient/FortiAuthenticator protocol 106
Configuration lock 108
FortiTray 108
Connecting to VPN connections 109
Diagnostic Tool 110
Custom FortiClient Installations 112
Download the license file 112
Prepare configuration files 113
Retrieve FortiClient configuration files 113
Configure Telemetry Gateway IP Lists 114
Create a custom installer 115
FortiClient (Windows) Configurator tool 116
FortiClient (Mac OS X) Configurator tool 120
Custom installation packages 122
FortiClient (Windows) 122
Advanced FortiClient profiles 123
Appendix A - Deployment Scenarios 124
Basic FortiClient profile 124
Advanced FortiClient profile 124
Use Active Directory Groups 125
Monitor connected users 125
Customize FortiClient using XML settings 125
Silent connection 126
Disable disconnect 126
Put it together 126
Appendix B - FortiClient API 127
Overview 127
API reference 127
Appendix C - Rebrand FortiClient 129
Appendix D - FortiClient Log Messages 134
Appendix E - Vulnerability Patches 146
Automatic vulnerability patching 146
Manual vulnerability patching 146

Change Log

Date	Change Description
2017-03-09	Initial release of FortiClient 5.4.3.
2017-05-03	Add back the following missing topic: Save password, auto connect, and always up on page 88
2017-05-12	Updated to clarify that only the AntiVirus feature is supported on Windows servers.

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This document was written for FortiClient (Windows) 5.4.3. Not all features described in this document are supported for FortiClient (Mac OS X) 5.4.3.

FortiClient modes and features

FortiClient offers two licensing modes: Standalone mode and Managed mode. The standalone mode is free, and the managed mode is licensed. In managed mode, FortiClient is used with FortiGate, FortiClient Enterprise Management Server (EMS), or both FortiGate and EMS.

The following table provides a feature comparison between standalone FortiClient (free version) and managed FortiClient (licensed version).

Standalone FortiClient (Free)	Managed FortiClient (Licensed)
Installation Options • Complete: All Endpoint Security and VPN components will be installed. • VPN Only: only VPN components (IPsec and SSL) will be installed.	**Installation Options** • Complete: All Endpoint Security and VPN components will be installed. • VPN Only: only VPN components (IPsec and SSL) will be installed. • Create a custom FortiClient installer using the FortiClient Configurator tool.
Threat Protection • Real-time Antivirus Protection • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware)	**Threat Protection** • Real-time Antivirus Protection • FortiSandbox support • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware) • Integration with FortiSandbox
Web Content • Web Filtering • YouTube Education Filter	**Web Content** • Web Filtering • YouTube Education Filter

Standalone FortiClient (Free)	Managed FortiClient (Licensed)
VPN • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Elliptical Curve Certificate Support • Two-Factor Authentication	**VPN** • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Elliptical Curve Certificate Support • Two-Factor Authentication
Logging • VPN, Antivirus, Web Security, and Update Logging • View logs locally	**Logging** • VPN, Application Firewall, Antivirus, Web Filter, Update, and Vulnerability Scan Logging • View logs locally
	Network Access Compliance • Compliance • Define and enforce enterprise security policies when FortiClient used with FortiGate.
	Application Control • Application Firewall • Block Specific Application Traffic
	Vulnerability Management • Vulnerability Scan • Link to FortiGuard with information on the impact and recommended actions • Receive remediation instructions for addressing endpoint vulnerabilities, including access to software patches
	Central Management • Centralized FortiClient monitoring with FortiGate or EMS • Centralized configuration provisioning and deployment with EMS
	Central Logging • Upload logs to FortiAnalyzer or FortiManager. FortiClient must connect to FortiGate or EMS to upload logs to FortiAnalyzer or FortiManager.

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or EMS. In this mode, FortiClient is free both for private individuals and commercial businesses to use; no license is required. See Standalone FortiClient on page 25.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

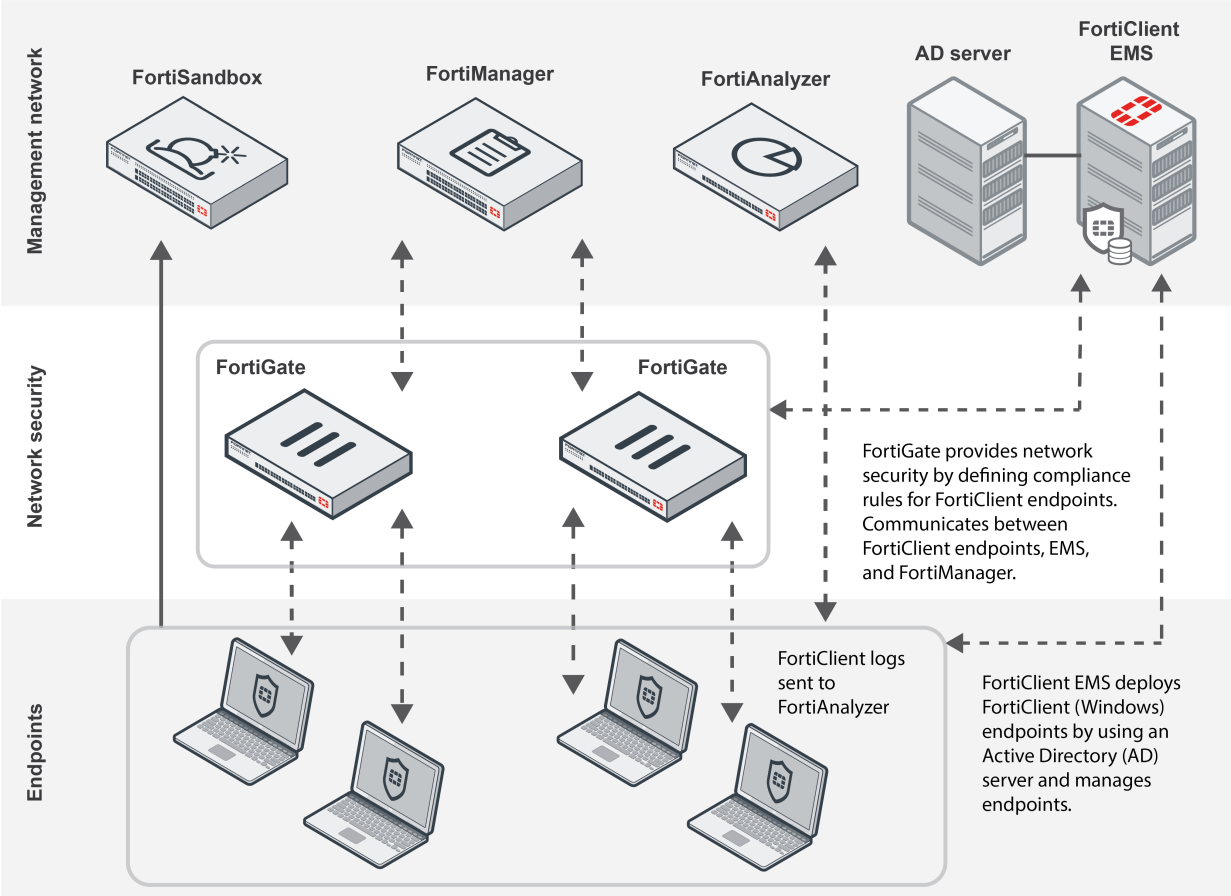
Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to FortiGate or EMS. In this mode, FortiClient licensing is applied to FortiGate or EMS. No separate license is required on FortiClient itself. See Managed FortiClient on page 26.

FortiClient supports endpoint compliance only when FortiClient Telemetry is connected to FortiGate.

Fortinet product support for FortiClient

The following Fortinet products work together to support FortiClient in managed mode:

- FortiClient EMS
- FortiManager
- FortiGate
- FortiAnalyzer
- FortiSandbox



FortiClient EMS

FortiClient EMS runs on a Windows server. EMS can manage FortiClient endpoints by deploying FortiClient (Windows) and profiles to endpoints, and the endpoints can connect FortiClient Telemetry to FortiGate or EMS. FortiClient endpoints connect to FortiGate to participate in Security Fabric or compliance enforcement. FortiClient endpoints connect to EMS to be managed in real time.

For information on EMS, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

FortiManager

FortiManager provides central FortiClient management for FortiGate devices that are managed by FortiManager. In FortiManager, you can create one or more FortiClient profiles that you can assign to multiple FortiGate devices. You can also import FortiClient profiles from one FortiGate device and assign the FortiClient profile to other FortiGate devices. When FortiClient endpoints are connected to managed FortiGate devices, you can use FortiManager to monitor FortiClient endpoints from multiple FortiGate devices.

For information on FortiManager, see the *FortiManager Administration Guide*, available in the Fortinet Document Library.

FortiGate

FortiGate provides network security. FortiGate devices define compliance rules for NAC (network access control) for connected FortiClient endpoints, and FortiClient communicates the compliance rules to endpoints. FortiGate devices communicate between FortiClient endpoints, EMS, and FortiManager, when FortiManager is used.

When FortiClient Telemetry is connected to FortiGate, endpoints can participate in Security Fabric or compliance enforcement.

For information on FortiGate, see the *FortiOS Handbook*, available in the Fortinet Document Library.

FortiAnalyzer

FortiAnalyzer can receive logs from FortiClient endpoints that are connected to FortiGate or EMS, and you can use FortiAnalyzer to analyze the logs and run reports. FortiAnalyzer receives logs directly from FortiClient. However, in FortiAnalyzer, you view FortiClient logs under the device to which the FortiClient endpoint is connected. For example, when FortiClient endpoints are connected to FortiGate devices, you must add the FortiGate devices to FortiAnalyzer to view FortiClient logs for the FortiClient endpoints that are connected to FortiGates.

For information on FortiAnalyzer, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

FortiSandbox

FortiSandbox offers the capabilities to analyze new, previously unknown, and undetected virus samples in realtime. Files sent to it are scanned first, using similar Antivirus (AV) engine and signatures as are available on FortiOS and FortiClient. If the file is not detected but is an executable file, it is run in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behavior in the VM.

FortiClient integration with FortiSandbox allows users to submit files from removable media or the network to FortiSandbox for automatic scanning. When configured, FortiClient will send supported files downloaded over the internet to FortiSandbox if they cannot be detected by the local, real-time scanning. Access to the downloaded file can be blocked until the scanning result is returned.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all real-time and on-demand AV scanning.

For more information, see the *FortiSandbox Administration Guide*, available in the Fortinet Document Library.

This feature requires a FortiSandbox running version 2.1 or newer and is only available on FortiClient (Windows).

Licensing

FortiClient managed mode requires a license. In managed mode, FortiClient licensing is applied to FortiGate or EMS.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses for FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses for EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Installation requirements

The following table lists operating system support and the minimum system requirements.

Operating System Support	Minimum System Requirements
• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit)	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.

Operating System Support	Minimum System Requirements
• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.
• Mac OS X v10.8 Mountain Lion • Mac OS X v10.9 Mavericks • Mac OS X v10.10 Yosemite • Mac OS X v10.11 El Capitan • Mac OS X v 10.12 Sierra	• Apple Mac computer with an Intel processor • 256MB of RAM • 20MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

Windows XP (32-bit) is supported when FortiClient software updates are disabled. You can disable FortiClient software updates by using EMS or FortiClient XML. Signature updates remain supported when FortiClient software updates are disabled.

For Windows servers, only the AntiVirus feature for FortiClient is supported.

Firmware images and tools

Microsoft Windows

The following files are available in the firmware image file folder:

- FortiClientSetup_5.4.xx.xxxx.exe
  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.4.xx.xxxx.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_5.4.xx.xxxx_x64.exe
  Standard installer for Microsoft Windows (64-bit).

- FortiClientSetup_5.4.xx.xxxx_x64.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_5.4.xx.xxxx.zip
  A zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files:

The following tools and files are available in the FortiClientTools_5.4.xx.xxxx.zip file:

- FortiClientConfigurator
  An installer repackaging tool that is used to create customized installation packages.
- FortiClientVirusCleaner
  A virus cleaner.
- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- SSLVPNcmdline
  Command line SSL VPN client.
- SupportUtils
  Includes diagnostic, uninstallation, and reinstallation tools.
- VPNAutomation
  A VPN automation tool.

When creating a custom FortiClient 5.4 installer by using the FortiClient Configurator tool, you can choose which features to install. You can also select to enable or disable software updates, configure SSO, and rebrand FortiClient.

Mac OS X

The following files are available in the firmware image file folder:

- FortiClient_5.4.x.xxx_macosx.dmg
  Standard installer or Mac OS X.
- FortiClientTools_5.4.x.xxx_macosx.tar
  FortiClient includes various utility tools and files to help with installations.

The following tools and files are available in the FortiClientTools `.tar` file:

- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- FortiClientConfigurator
  An installer repackaging tool that is used to create customized installation packages.
- RebrandingResources
  Rebranding resources used by the FortiClient Configurator tool.

When creating a custom FortiClient 5.4.3 installer by using the FortiClient Repackager tool, you can choose to install Everything, VPN Only, or SSO only. You can also select to enable or disable software updates and rebrand FortiClient.

FortiClient 5.4 cannot use FortiClient version 5.0 licenses. To use FortiClient Configurator, you need to use the FortiClient version 5.4 license file.

What's New in FortiClient 5.4

The following is a list of new features and enhancements in FortiClient 5.4.

This document was written for FortiClient (Windows) 5.4.3. Not all features described in this document are supported for FortiClient (Mac OS X) 5.4.3.

FortiClient 5.4.3

There are no new features in FortiClient 5.4.3.

FortiClient 5.4.2

The following is a list of new features in FortiClient version 5.4.2.

- FortiClient (Mac OS X) supports macOS Sierra (version 10.12).
- FortiClient in standalone mode no longer includes a banner at the bottom of the console.

FortiClient 5.4.1

The following is a list of new features in FortiClient version 5.4.1.

Endpoint control

FortiClient Telemetry

FortiClient Telemetry is the new name of the connection between FortiClient and FortiGate or EMS. You no longer register FortiClient endpoints to FortiGate or EMS, but connect FortiClient Telemetry to FortiGate or EMS. See FortiClient Telemetry Connection on page 49.

Endpoint compliance

FortiClient includes a *Compliance* tab that communicates whether FortiClient is connected to FortiGate or EMS and whether the endpoint is compliant.

When connected to FortiGate, the *Compliance* tab communicates whether FortiClient and the endpoint device are compliant with the compliance rules defined by FortiGate. Endpoint users can view the *Compliance* tab to review compliance rules and status. Endpoint users can also view information about steps required to remain compliant with the network access rules. See Compliance on page 52.

Picture of endpoint user

FortiClient can now display a small picture of the endpoint user on the *Compliance* tab. This feature is available when FortiClient is used with EMS, and the feature is enabled in EMS. When enabled, FortiClient uses the picture defined in the Windows operating system on the endpoint device. FortiClient displays no picture when no picture is found in the Windows operating system.

FortiClient Telemetry can also send the picture to FortiGate and EMS.

FortiGate endpoint control

FortiGate 5.4.1 has changed how it works with FortiClient endpoints. Now FortiGate is used to define the compliance rules for NAC in a FortiClient profile, and FortiClient helps to enforce the rules on endpoints. When you use FortiGate to create a FortiClient profile, you define the compliance rules, and you specify how to handle non-compliant FortiClient endpoints. Non-compliant endpoints can be blocked from network access, warned about non-compliance while maintaining network access, or automatically updated to maintain network access. See About managed mode on page 26.

FortiGate endpoint control requires FortiOS 5.4.1 and FortiClient 5.4.1.

Improved installation process for FortiClient (Windows)

An upgrade schedule dialog box is displayed in advance when deploying FortiClient from EMS to endpoints running Windows operating system. If no FortiClient is installed on the endpoint, no reboot is required for the installation, and no upgrade schedule dialog box is displayed. The user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog box is displayed with a 15 minute warning.

Vulnerability scan

The Vulnerability scan feature requires specific versions of products. If you are using FortiGate, FortiOS 5.4.1 is required. If you are using FortiClient EMS, version 1.0.1 is required.

Vulnerability scan enhancements

Vulnerability scan feature in FortiClient (Windows) can perform a full scan of the endpoint to find any OS, Microsoft Office, browser and third-party vulnerabilities. FortiClient can then report the vulnerabilities to FortiAnalyzer and FortiGate or FortiClient EMS, depending on whether FortiClient is connected to FortiGate or FortiClient EMS. See Vulnerability Scan on page 94.

Vulnerability auto-patching

FortiClient (Windows) supports automatic patching of vulnerabilities where FortiClient will initiate and apply any updates required to resolve detected vulnerabilities and return endpoints to a secure state. See Vulnerability Scan on page 94.

FortiSandbox support for removable media

Files on removable media can now be sent for on-demand FortiSandbox scanning. You can configure FortiSandbox to scan files on removable media by using FortiClient XML. For more information, see the *FortiClient XML Reference*.

Configurator tool

You can now use the FortiClient Configurator tool to add a Telemetry Gateway IP List to a custom FortiClient installer. See Custom FortiClient Installations on page 112.

FortiClient 5.4.0

The following is a list of new features in FortiClient version 5.4.0.

Antivirus

Advanced Persistent Threats

FortiClient 5.4.0 has enhanced capabilities for the detection of Advanced Persistent Threats (APT). There are two changes added in this respect:

- Botnet Command and Control Communications Detection
- FortiSandbox integration (Windows only)

Botnet Communication Detection

Botnets running on compromised systems usually generate outbound network traffic directed towards Command and Control (C&C) servers of their respective owners. The servers may provide updates for the botnet, or commands on actions to execute locally, or on other accessible, remote systems. When the new botnet feature is enabled, FortiClient monitors and compares network traffic with a list of known Command and Control servers. Any such network traffic will be blocked.

FortiSandbox Integration

FortiSandbox offers the capabilities to analyze new, previously unknown and undetected virus samples in real-time. Files sent to it are scanned first, using similar Antivirus (AV) engine and signatures as are available on the FortiOS and FortiClient. If the file is not detected but is an executable file, it is run (sandboxed) in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behavior in the VM.

FortiClient integration with FortiSandbox allows users to submit files to FortiSandbox for automatic scanning. When configured, FortiClient will send supported files downloaded over the internet to FortiSandbox if they cannot be detected by the local, real-time scanning. Access to the downloaded file is blocked until the scanning result is returned.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all real-time and on-demand AV scanning.

This feature requires a FortiSandbox running version 2.1 or newer and is only available on FortiClient (Windows).

Enhanced Real-Time Protection Implementation

The Real-Time Protection (RTP) or on-access feature in FortiClient uses tight integration with Microsoft Windows to monitor files locally, or over a network file system, as they are being downloaded, saved, run, copied, renamed, opened, or written to. The FortiClient driver coupling with Windows has been re-written to use modern APIs provided by Microsoft. All basic features remain the same, with a few minor differences in behavior. Some noticeable performance enhancements could be observed in various use case scenarios.

This feature is only available on FortiClient (Windows).

Web Filtering

Web Browser Usage and Duration

If configured, FortiClient will record detailed information about the user's web browser activities, such as:

- A history of websites visited by the user (as shown in regular web browser history)
- An estimate of the duration or length of stay on the website.

These logs are sent to FortiAnalyzer, if configured. With FortiAnalyzer 5.4.0 or newer, the FortiClient logs sent from various endpoints may be viewed in FortiView.

This feature requires FortiAnalyzer 5.4.0 or newer.

VPN

Authorized Machine Detection

For enterprises where new computers may be brought into the organization by employees, FortiClient can be configured to check or identify the computer before allowing it to establish IPsec VPN or SSL VPN connections to the FortiGate. The administrator may configure restrictions with one or more of the following:

- Registry check: Ensure a specific registry path contains a predetermined value
- File check: Verify the existence of a specific file at a specified location
- Application check: Ensure that a specific application is installed and running

The verification criteria can be configured using advanced FortiClient XML configurations on the FortiGate or FortiClient Enterprise Management Server (EMS).

This feature only applies to FortiClient (Windows).

New SSL VPN Windows driver

The FortiClient SSL VPN driver `pppop.sys` was re-written to use the latest Microsoft recommended CoNDIS WAN driver model. The new driver is selected when FortiClient is installed on Windows 7 or newer. The SSL VPN driver included in the previous versions of FortiClient will still be maintained.

This feature only applies to FortiClient (Windows).

New IPsec VPN Windows drivers

FortiClient IPsec VPN drivers have been updated to support Microsoft Windows NDIS 6.3 specification. The new drivers are compatible with Microsoft Windows 8.1 or newer.

This feature only applies to FortiClient (Windows).

Support for DTLS

FortiClient SSL VPN connections to FortiGate now support Datagram Transport Layer Security (DTLS) by using User Datagram Protocol (UDP) as the transport protocol. Previously FortiClient SSL VPN connections supported only Transport Control Protocol (TCP). You can now use FortiGate to configure SSL VPN connections that use DTLS. You cannot use FortiClient to configure SSL VPN connections that use DTLS. When FortiClient endpoints use a DTLS-enabled SSL VPN connection with FortiGate, and FortiGate communicates DTLS support, FortiClient uses DTLS via UDP. If DTLS fails, FortiClient will fall back to use TLS to establish an SSL VPN connection.

This feature only applies to FortiClient (Windows).

Endpoint Control

Integration with the new FortiClient EMS

FortiClient Enterprise Management Server (EMS) is a new product from Fortinet for businesses to use to manage their computer endpoints. It runs on a Windows Server, not requiring a physical Fortinet device. Administrators may use it to gain insight into the status of their endpoints. The EMS supports devices running Microsoft Windows, Mac OS X, Android, and iOS.

FortiClient Endpoint Control (EC) protocol has been updated to seamlessly integrate with FortiClient EMS. Various changes were added to support EMS features, including:

- Deployment of FortiClient to new Microsoft Windows devices
- Continuous monitoring of device statuses
- AV engine and signature update status reports

- AV scanning schedules and requests for AV scans
- Notifications about protection statuses.

FortiGate Network Access Control when FortiClient is Deployed using EMS

The new EMS can be used to deploy FortiClient to a large number of Microsoft Windows endpoints. While creating a profile for FortiClient deployment, the EMS administrator can choose to configure the FortiClient to register to the same EMS, or to a FortiGate.

Changes in FortiClient 5.4.0 allow the EMS administrator to deploy FortiClient to endpoints, and configure it to register to a FortiGate, while simultaneously notifying the EMS of its registration status. The FortiClient EC registration to the FortiGate is required for Network Access Compliance (NAC). The administrator can configure the FortiGate to allow access to network resources only if the client is compliant with the appropriate interface EC profile.

EMS can only deploy FortiClient to endpoint devices that are running Microsoft Windows. This feature requires FortiOS 5.4.0 or newer.

Quarantine an Infected Endpoint from the FortiGate or EMS

A computer endpoint that is considered to be infected may be quarantined by the FortiGate or EMS administrator. FortiClient needs to be online, using FortiClient EC protocol, and registered to the FortiGate or EMS.

Once quarantined, all network traffic to or from the infected endpoint will be blocked locally. This allows time for remediation actions to be taken on the endpoint, such as scanning and cleaning the infected system, reverting to a known clean system restore point, or re-installing the operating system.

The administrator may un-quarantine the endpoint in the future from the same FortiGate or EMS.

This feature requires FortiOS 5.4.0 or newer or FortiClient EMS 1.0 or newer.

Importing FortiGate CA Certificate after EC Registration

When the FortiGate is configured to use SSL deep inspection, users visiting encrypted websites will usually receive an invalid certificate warning. The certificate signed by the FortiGate does not have a Certificate Authority (CA) at the endpoint to verify it. Users can manually import the FortiGate CA certificate to stop the error from being displayed; however, all users will have to do the same.

When registering FortiClient to a FortiGate, the FortiClient will receive the FortiGate's CA certificate and install it into the system store. If Firefox is installed on the endpoint, the FortiGate's CA certificate will also be installed into the Firefox certificate store. This way the end user will no longer receive the invalid certificate error message when visiting encrypted websites.

FortiGate CA certificates will be removed from the system store if FortiClient is uninstalled.

Enhancement to On-net/Off-net Configuration

The on-net feature requires the use of a FortiGate as a DHCP server. This is usually configured on the same FortiGate that the FortiClient will be registered. When the device that FortiClient is running on has an IP address from the FortiGate's DHCP server, it is on-net. For any other IP addresses, it is off- net.

There is a new way to configure the on-net feature. On the FortiGate, the DHCP server can be used, or several network subnets can be provided.

FortiClient will be on-net if:

- It is registered using EC to the FortiGate,
- It belongs to one of the pre-configured on-net subnets, or
- It provides the DHCP for on-net properties.

Otherwise, FortiClient will be off-net.

FortiClient GUI

Antivirus Settings Page

With the introduction of botnet detection, and the integration with FortiSandbox with FortiClient (Windows), the AV settings page on the FortiClient GUI has been updated to allow configuration of the new features. The AV settings page is accessible from the FortiClient dashboard. Select the AV tab on the left pane. Then click the settings icon on Real-Time Protection in the right pane.

The following may be selected on the AV settings page:

- File scanning (previously, Real-Time Protection or RTP)
- Scan unknown, supported files using FortiSandbox (Windows only)
- Malicious website detection
- Botnet detection (block known communication channels)

To use FortiSandbox , file scanning must be enabled (Windows only).

FortiClient Banner Design

If FortiClient (full version or VPN only) is running in standalone mode and not registered to a FortiGate or EMS, a single banner at the bottom of the GUI is displayed. When registered to a FortiGate or EMS, the banner is hidden by default. Similarly, when created from a FortiClient Configurator (Windows) or Repackager (OS X), no banner is displayed by default.

Logging

Enhancement to FortiClient logs

FortiClient will create a log entry to show just the URL visited by the user through a web browser. This is in addition to the network level logs generated by FortiClient.

Standalone FortiClient

About standalone mode

In standalone mode, FortiClient software is installed to computers or devices that have Internet access and are running a supported operating system. After FortiClient is installed, FortiClient automatically connects to FortiGuard Center (http://www.fortiguard.com) to protect the computer or device.

Get started

In standalone mode, you can configure FortiClient settings by using the FortiClient console. This section provides an overview of provisioning, configuring, and using FortiClient in standalone mode.

Provision and configure

In standalone mode, you can install FortiClient software to computers or devices with Internet access and configure a number of settings.

To provision and configure FortiClient:

1. Install FortiClient on computers or devices. See FortiClient Provisioning on page 42.
   FortiClient connects to the Fortinet FortiGuard server to protect the computer.
2. Configure FortiClient settings. See Settings on page 101.
3. Configure Antivirus settings. See Antivirus on page 63.
4. (Optional) Configure remote access. See IPsec VPN and SSL VPN on page 82.

Use FortiClient console

In standalone mode, you can use the following tabs in FortiClient console:

- Antivirus
- Web Security
- Remote Access

The *Compliance* tab is used only when FortiClient is running in managed mode. See Managed FortiClient on page 26.

To use the FortiClient console:

1. View Antivirus threats. See View scan results on page 69.
2. View web security results. See View violations on page 78.
3. Use remote access. See Add new connections on page 82.
4. View notifications. See View notifications on page 62.

Managed FortiClient

About managed mode

In managed mode, FortiClient software is installed to computers or devices on your network that have Internet access and are running a supported operating system. The computers or devices are referred to as FortiClient endpoints. After FortiClient software is installed on endpoint devices, FortiClient:

- Automatically connects to FortiGuard Center (http://www.fortiguard.com) to protect the endpoint
- Automatically attempts to connect FortiClient Telemetry to FortiGate or EMS

The endpoint user confirms the request to complete the FortiClient Telemetry connection to FortiGate or EMS.

> You can optionally configure a FortiClient Telemetry connection that requires no confirmation by the endpoint user. See Custom FortiClient Installations on page 112.

After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient receives a profile from FortiGate and/or EMS, and the endpoint is managed.

FortiClient profiles

When FortiClient is in managed mode, a profile is used to communicate compliance rules and to configure FortiClient software on endpoints. The content of the profile depends on whether FortiGate or EMS provides the profile.

FortiGate and compliance rules

In FortiGate, you can use a FortiClient profile to achieve the following goals:

- Define compliance rules for endpoint access to the network through FortiGate
- Define the non-compliance action—that is, how endpoints are handled that fail to comply with compliance rules
- (Optional) Define some configuration settings for FortiClient software on endpoints

Compliance rules

FortiGate compliance rules are used to define what configuration FortiClient software must have for the endpoint to maintain access to the network through FortiGate. The following is a sample of the compliance rules that you can enable or disable by using the FortiOS GUI:

- Antivirus
- Web filter
- Application firewall
- Vulnerability scan
- FortiClient software specific version

You can also define additional compliance rules by using the FortiOS CLI.

Non-compliance action

In FortiGate, you can use the profile to define how FortiClient endpoints are handled that fail to comply with the compliance rules. You can block, warn, or automatically update FortiClient endpoints. You set the rules by using FortiGate, and both FortiGate and FortiClient enforce the rules.

Both FortiGate and FortiClient enforce compliance rules for FortiClient 5.4.1 and later endpoints. FortiGate enforces compliance for FortiClient 5.4.0 and earlier endpoints, and for all versions of unregistered/unconnected FortiClient endpoints.

Following is a description of how each setting affects FortiClient endpoints:

- Block
  When FortiClient endpoints fail to comply with compliance rules, FortiClient blocks endpoint access to the network. Non-compliance information is displayed in the FortiClient console. The administrator or endpoint user is responsible for reading the noncompliance information and updating FortiClient software on the endpoint to adhere to the compliance rules. In this case, endpoint users can edit settings in the FortiClient console that are not controlled by the compliance rules or EMS.
- Warn
  When FortiClient endpoints fail to comply with compliance rules, FortiClient warns the endpoint users, but allows the endpoint user to access the network. Non-compliance information is displayed in the FortiClient console. The administrator or endpoint user is responsible for reading the non-compliance information and updating FortiClient software on the endpoint to adhere to the compliance rules. In this case, endpoint users can edit settings in the FortiClient console that are not controlled by the compliance rules or EMS.
- Auto-update
  FortiGate provides the compliance rules and some configuration information for FortiClient software that helps FortiClient and the endpoint remain compliant. However FortiClient endpoints can fail to comply with compliance rules because FortiGate cannot automatically update all aspects of the compliance rules, such as the required version of FortiClient or the operating system on the endpoint. FortiGate displays non-compliance information in the FortiOS GUI. The FortiGate administrator and endpoint user are responsible for reading the non-compliance information and keeping FortiClient endpoints compliant. In this case, most settings in FortiClient console are read-only. However, the endpoint user can edit some settings.

FortiClient configuration

When you use FortiGate to configure a FortiClient profile with a non-compliance setting of auto-update, the FortiClient profile can include configuration information for FortiClient software, which helps the FortiClient endpoint remain compliant with the compliance rules.

You can specify the following configuration information for FortiClient software:

- AntiVirus
- Web Filter
- Application Firewall
- Vulnerability Scan
- System Compliance

When the FortiClient endpoint receives the configuration information from FortiGate in the FortiClient profile, the settings in FortiClient console are automatically updated. Most settings in FortiClient console are read-only when

FortiGate provides the FortiClient profile. However, the endpoint user can change settings in FortiClient console that are not controlled by the FortiClient profile.

For more information about configuring FortiClient profiles by using FortiGate, see the *FortiOS Handbook*, available in the Fortinet Document Library.

CLI only

When using FortiGate to create FortiClient profiles, some settings can be configured only by using the FortiOS CLI. You must use the CLI to configure the following options:

- Allowed operating system for FortiClient endpoints
- Required third-party applications for FortiClient endpoints
- Registry entries for FortiClient endpoints
- File in the file system on FortiClient endpoints

For more information, see the *CLI Reference for FortiOS*.

EMS and profiles

In FortiClient EMS, a profile is used to install FortiClient on endpoint devices and/or define the configuration for FortiClient software on endpoint devices. The profile consists of the following sections:

- FortiClient Installer
- Antivirus
- Web Filtering
- Application Firewall
- VPN
- Vulnerability Scan
- System Settings

When the FortiClient endpoint receives the configuration information in the FortiClient profile, the settings in FortiClient console are automatically updated. Settings are locked and read-only when EMS provides the configuration in a profile.

For more information about configuring profiles by using FortiClient EMS, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

FortiClient Telemetry connection options

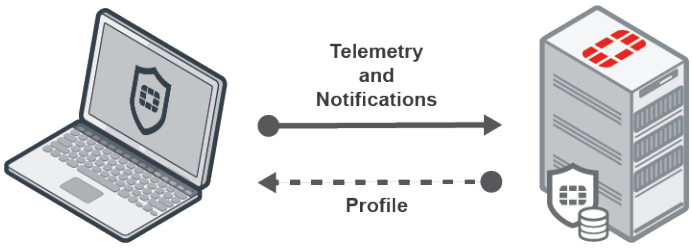
FortiClient Telemetry supports the following connection options:

- FortiClient EMS on page 29
- FortiGate on page 29
- FortiGate and EMS integration on page 29

EMS manages FortiClient endpoints by using the FortiClient Telemetry connection. Endpoints connect FortiClient Telemetry to FortiGate to participate in Security Fabric or compliance enforcement. FortiGate units do not manage endpoints.

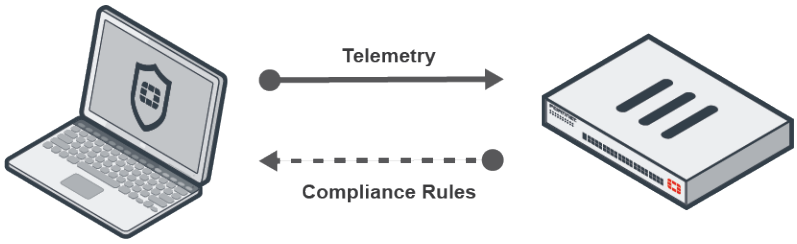
FortiClient EMS

In this configuration, FortiClient Telemetry connects to EMS, and EMS pushes a profile to FortiClient. The profile contains the configuration information for FortiClient. EMS manages FortiClient endpoints.



FortiGate

In this configuration, FortiClient Telemetry is connected to FortiGate, and FortiClient downloads a profile from FortiGate. The profile contains the compliance rules and optionally some configuration information for FortiClient.



FortiGate and EMS integration

In this configuration, FortiClient Telemetry connects to FortiGate for NAC and EMS for management. This configuration is sometimes called integrated mode.

When FortiClient Telemetry is connected to FortiGate, FortiClient downloads a profile from FortiGate. The profile contains the compliance rules and optionally some configuration information for FortiClient, depending on the *Non-compliance action* setting in the profile. The *Non-compliance action* setting affects FortiClient as follows:

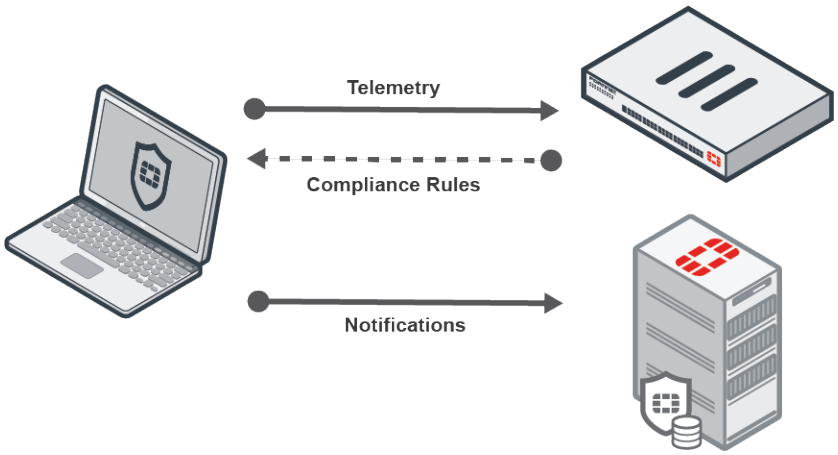
- When the *Non-compliance action* setting is *Auto-update*, only the profile from FortiGate is downloaded to FortiClient. EMS cannot push a profile of configuration information to FortiClient.
- When the *Non-compliance action* setting is *Block* or *Warning*, the profile from FortiGate is downloaded to FortiClient. EMS can also push a profile of configuration information to FortiClient. The profile from EMS is optional and in addition to the profile from FortiGate.

If the non-compliance action is set to block or warning in the FortiClient profile created by using FortiGate, FortiGate does not provision the FortiClient endpoint, and you must manually configure FortiClient or configure FortiClient by using EMS. If the non-compliance action is set to auto-update, FortiGate attempts to provision FortiClient endpoints to be compliant with the compliance rules.

FortiClient Telemetry connection when non-compliance action is set to auto-update

Following is a summary of how the FortiClient Telemetry connection works when the *Non-compliance action* setting is *Auto-update* in the profile from FortiGate:

- FortiClient Telemetry connects to FortiGate, and FortiClient sends notifications to EMS.
- FortiClient downloads a profile from FortiGate. The profile contains compliance rules and some configuration information.

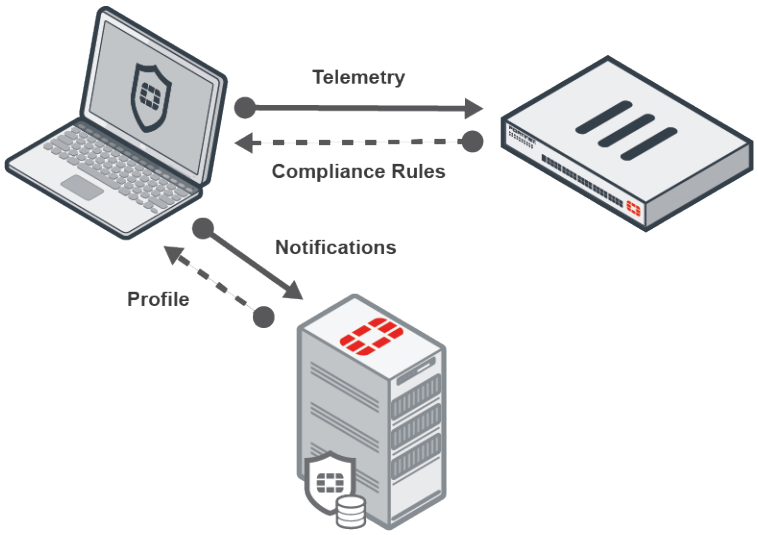


FortiClient Telemetry connection when non-compliance action is set to block or warn

Following is a summary of how the FortiClient Telemetry connection works when the *Non-compliance action* setting is *Block* or *Warn* in the profile from FortiGate:

- FortiClient Telemetry connects to FortiGate, and FortiClient sends notifications to EMS.
- FortiClient downloads a profile from FortiGate. The profile contains compliance rules.
- (Optional) EMS pushes a profile to FortiClient. The profile contains configuration information.

You should ensure that the configuration pushed from EMS matches the compliance rules set on FortiGate to avoid conflicting settings.



Telemetry Gateway IP Lists

The Telemetry Gateway IP List is a list of gateway IP addresses that FortiClient in managed mode can use to connect FortiClient Telemetry to FortiGate or EMS. After FortiClient installation completes on the endpoint device, FortiClient automatically launches and uses the Telemetry Gateway IP List to locate FortiGate and/or EMS for FortiClient Telemetry connection.

After FortiClient is installed on the endpoint and FortiClient Telemetry is connected to FortiGate and/or EMS, you can view the Telemetry Gateway IP List in the FortiClient console. See View gateway IP lists on page 57.

Configure Telemetry Gateway IP Lists (EMS)

FortiClient EMS includes the option to create one or more Telemetry Gateway IP Lists. The list can include IP addresses for EMS and for FortiGate. You can assign Telemetry Gateway IP Lists to domains and workgroups in EMS. You can also update the assigned Telemetry Gateway IP Lists after FortiClient is installed, and the updated lists are pushed to FortiClient endpoints. See the *FortiClient EMS Administration Guide*.

Configure Telemetry Gateway IP Lists (FortiGate)

If you are using FortiGate without EMS, you can add Telemetry Gateway IP addresses to the FortiClient installer by using the Configurator Tool. See Custom FortiClient Installations on page 112.

On-net / off-net status with FortiGate and EMS

Endpoints must connect FortiClient Telemetry to FortiGate or EMS for FortiClient console to display an on-net, off-net, or offline status. You can view the on-net/off-net status on the *Compliance* tab in FortiClient console. See View user details on page 56.

The following rules identify when FortiGate, EMS, or FortiClient determine the status:

- When endpoints connect FortiClient Telemetry to FortiGate or EMS, FortiGate or EMS determines whether the endpoint has an on-net or off-net status.
- When endpoints cannot connect FortiClient Telemetry to FortiGate or EMS, FortiClient determines the on-net or off-net status, based on the on-net subnets.

When FortiGate and EMS are integrated, the primary FortiClient Telemetry connection is to FortiGate, and FortiGate calculates the status.

FortiGate

The version of FortiClient and FortiOS do not affect the on-net, off-net, or online status. The following examples show how FortiGate determines the status for the endpoint:

- The endpoint has a status of on-net when the endpoint is behind a FortiGate, and the endpoint receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- The endpoint has a status of on-net when the endpoint is inside one of the on-net subnets defined by FortiGate. You can configure on-net subnets in the FortiClient profile by using the FortiOS CLI and the `set on-net addr` command.
- The endpoint has a status of off-net when the endpoint is outside of the FortiGate network, such as connected through an external interface or hasn't received option 224 with the FortiGate serial number.

- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to FortiGate, and the endpoint is outside one of the on-net networks, even when option 224 and the FortiGate serial number are configured.
- The endpoint has a status of offline on-net when the endpoint is inside one of the on-net networks, but cannot connect FortiClient Telemetry to FortiGate.

For FortiClient to be in an on-net network, the IP address of FortiGate or EMS should be routed via the IP address from the on-net network.

EMS

The version of FortiClient and EMS do not affect the on-net, off-net, or online status. The following table shows how various configurations determine the status for the endpoint when FortiClient Telemetry is connected to EMS:

EMS DHCP On-net / Off-net Setting	On-net Subnet	Option 224 Serial Number	Endpoint Status
Off	No	N/A	On-net
On	No	Option not configured	Off-net
On	No	Option configured	On-net
Off or on	Yes and match	Configured or not	On-net
Off or on	Yes and do not match	Configured or not	Off-net

The following examples show how EMS determines the status for the endpoint:

- The endpoint has a status of offline when the endpoint cannot connect FortiClient Telemetry to EMS, and the endpoint is outside one of the on-net networks.
- The endpoint has a status of offline on-net when the endpoint cannot connect FortiClient Telemetry to EMS, but the endpoint is inside one of the on-net networks.

On-net subnets have higher priority over other settings. In addition, EMS doesn't compare the Option 224 serial number. As long as the endpoint has the serial number, EMS assumes that the endpoint is behind a FortiGate and is on-net.

Get started

This section provides an overview of how to configure, provision, and use FortiClient in managed mode.

Configure endpoint management

Before you can provision FortiClient in managed mode, you must configure FortiGate or EMS to manage FortiClient endpoints.

To configure endpoint management:

1. Configure the product or products that you will use to manage FortiClient endpoints.
   The following table identifies where to find instructions:

FortiGate	• Configure FortiGate endpoint control. See Configure FortiGate on page 34. For more information, see the *FortiOS Handbook*.
EMS	• Configure EMS. See the *FortiClient EMS Administration Guide*.
FortiGate integrated with EMS	• For FortiGate, configure endpoint control. See Configure FortiGate on page 34. For more information, see the *FortiOS Handbook*. • For EMS, see the *FortiClient EMS Administration Guide*.

After you configure EMS, FortiGate, or both FortiGate and EMS to manage FortiClient endpoints, you are ready to provision FortiClient.

Provision FortiClient

This section provides an overview of how to provision FortiClient in managed mode.

To provision FortiClient:

1. Ensure that you have EMS, FortiGate, or both FortiGate and EMS configured to manage FortiClient endpoints.
2. Provision FortiClient on endpoint devices with Internet access. See FortiClient Provisioning on page 42.
   You can use one of the following methods:
   - FortiClient EMS with a Microsoft Active Directory server
   - Microsoft Active Directory server

   After FortiClient installs, FortiClient Telemetry attempts connection to FortiGate or EMS. For more information, see FortiClient Telemetry Connection on page 49.

   After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient downloads a profile from FortiGate and/or EMS. The computer with FortiClient installed and FortiClient Telemetry connected is now a managed endpoint.
3. Manage endpoints by using EMS. You can also use FortiOS to monitor endpoints.

Use FortiClient console

This section describes how a FortiClient endpoint user can use the FortiClient console when FortiClient is managed by FortiGate and/or EMS.

To use the FortiClient console:

1. View FortiClient Telemetry connection status, last profile update, and the gateway IP list. See Compliance on page 52.
   If FortiClient Telemetry is connected to FortiGate, you can also view compliance status and instructions for remaining compliant on the *Compliance* tab.
2. View Antivirus threats. See Antivirus on page 63.
3. View web filter results. See View violations on page 78.

4. View application firewall results. See Application Firewall on page 80.
5. Configure and use remote access. See IPsec VPN and SSL VPN on page 82.
6. View vulnerability scan results. See Vulnerability Scan on page 94.
7. View notifications. See View notifications on page 62.

Configure FortiGate

This section provides an overview on FortiOS configuration for endpoint control.

Endpoint control is available on FortiGate 30D series devices and higher.

Endpoint control requires FortiClient 5.4.1 or later and either a FortiGate device running FortiOS 5.4.1 or later, or a server running FortiClient EMS 1.0 or later.

Get started

FortiGate endpoint control is configured by completing the following tasks by using FortiOS:

1. Enable the endpoint control feature. See Enable the Endpoint Control feature on page 34.
2. Enable FortiTelemetry on an interface. See Enable FortiTelemetry on an interface on page 34.
3. Configure firewall policies. See Configure firewall policies on page 35.
4. Configure FortiClient profiles. See Configure FortiClient profiles on page 36.

   After FortiClient software is installed on endpoints, and the FortiClient endpoints connect FortiTelemetry to FortiGate, FortiClient downloads a FortiClient profile from FortiGate.

Additional configuration options are available, depending on the needs of your network.

Enable the Endpoint Control feature

When using the GUI for configuration, you must enable endpoint control on FortiGate devices to use the device for FortiClient endpoint management.

When using the CLI for configuration, you can skip this step.

To enable the endpoint control feature:

1. Go to *System* > *Feature Select*.
2. In the *Security Features* list, enable *Endpoint Control*.
3. In the *Additional Features* list, enable *Multiple Security Profiles*.
4. Click *Apply*.

Enable FortiTelemetry on an interface

You must configure FortiClient communication on a FortiGate interface by specifying an IP address and enabling FortiTelemetry communication.

The IP address for the interface defines the gateway IP address for the FortiGate that FortiClient endpoints will use to connect FortiClient Telemetry to FortiGate.

You can also add any devices that are exempt from requiring FortiClient software to an exemption list for the interface.

To enable FortiTelemetry on an interface:

1. Go to *Network* > *Interfaces*.
2. Select an interface, and click *Edit*.
3. Set the following options:

Address	In the *IP/Network Mask*, type the gateway IP address.
Restrict Access	Beside *Administrative Access*, select the *FortiTelemetry* check box to enable endpoints to send FortiTelemetry to FortiGate.
Networked Devices	Enable *Device Detection* to allow FortiGate to detect the operating system on connected endpoint devices.
Admission Control	Enable *Enforce FortiTelemetry for All FortiClients* to require endpoint compliance for all endpoints.
	Click the *Exempt Sources* box, and add the devices that are exempt from requiring FortiClient software with a FortiClient Telemetry connection to the FortiGate, such as Linux PC. For example, FortiClient software currently does not support Linux operating system. You can add this type of device to the *Exempt Sources* list.
	Click the *Exempt Destinations/Services* box, and add the destinations and services.

4. Configure the remaining options as required.
5. Click *OK*.

Configure firewall policies

You must configure a firewall policy for FortiClient access to the Internet. The firewall policy must include the incoming interface that is defined for FortiTelemetry communication, and the outgoing interfaces that you want FortiClient endpoints to use for accessing the Internet. Otherwise, endpoints will be unable to access the Internet.

To configure firewall policies:

1. Go to *Policy & Objects* > *IPv4 Policy*.
2. Click *Create New* in the toolbar. The *New Policy* window is displayed.
3. In the *Name* box, type a name for the firewall policy.
4. In the *Incoming Interface* list, select the port defined for FortiTelemetry communication.
5. In the *Outgoing Interface*, select the port(s) defined for outgoing traffic from FortiGate.
6. Configure the remaining options as required.
7. Click *OK*.

Configure FortiClient profiles

FortiGate includes a default FortiClient profile. You can edit the default profile or create a new profile. FortiClient profiles are used to communicate compliance rules to FortiClient endpoints.

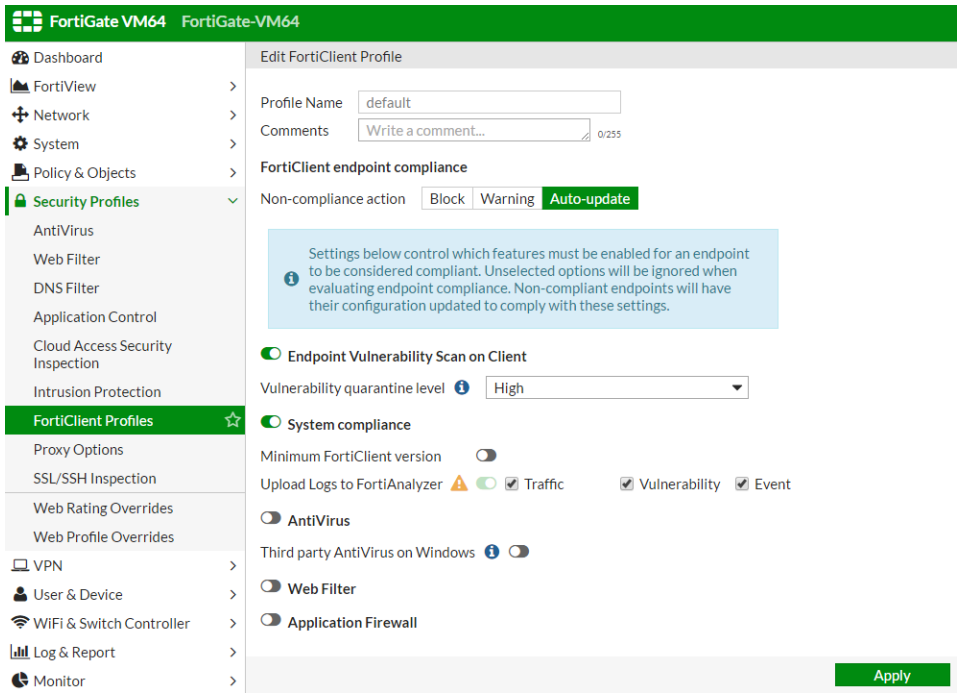
The option to assign the profile to device groups, user groups, and users is available only when you create a new FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication.

You must enable *Multiple Security Profiles* in the *System* > *Feature Select* pane to create a new FortiClient profile.

For more information about creating FortiClient profiles by using FortiGate, see the *FortiOS Handbook--Security Profiles*.

To configure FortiClient profiles:

1. Go to *Security Profiles* > *FortiClient Profiles*. You can edit the default profile or create a new FortiClient profile.



2. Set the following options:

Profile Name	Type a name for the profile.
Comments	Type comments about the profile.
Assign Profile To	Click to specify which devices, users, and addresses will receive the FortiClient profile. This option is available only when you enable multiple security profiles and create a new profile.

FortiClient endpoint compliance	Use the options in this section to specify how to handle FortiClient endpoints that fail to meet the compliance rules.
Non-compliance action	Select either *Block*, *Warning*, *Auto-update*. See also Non-compliance action on page 27.
Endpoint Vulnerability Scan on Client	You can enable or disable *Endpoint Vulnerability Scan on Client*. When enabled, FortiClient is required to have Vulnerability Scan enabled. When *Non-compliance action* is set to *Auto-update*, you can enable and configure *Endpoint Vulnerability Scan on Client* by using only FortiGate.
System Compliance	You can enable or disable *System Compliance*. When enabled, a minimum FortiClient version is required on endpoints. When *Non-compliance action* is set to *Auto-update*, you can enable and configure *Minimum FortiClient version* by using only FortiGate. You can also enable logging to FortiAnalyzer, and select what types of logs to send to FortiAnalyzer.
AntiVirus	You can enable or disable AntiVirus. When enabled, FortiClient console is required to have Antivirus enabled. When *Non-compliance action* is set to *Auto-update*, you can enable and configure AntiVirus by using only FortiGate.
Web Filter	You can enable or disable Web Filter and select a profile. When enabled, FortiClient is required to have Web Filter enabled. When *Non-compliance action* is set to *Auto-update*, you can enable and configure Web Filter by using only FortiGate.
Application Firewall	You can enable or disable Application Firewall and select a profile. When enabled, FortiClient is required to have Application Firewall enabled. When *Non-compliance action* is set to *Auto-update*, you can enable and configure Application Firewall by using only FortiGate.

3. Click *OK*.

Enable a key password for FortiTelemetry connection

You can configure a connection key password for FortiClient Telemetry connection to FortiGate devices. When connecting FortiClient Telemetry to FortiGate, the user must enter the connection key password in FortiClient console before the connection can be completed.

You must use the CLI to enable a key password.

To enable key password:

1. On your FortiGate device, go to *Dashboard* > *CLI Console*, and enter the following CLI command:

```
config endpoint-control settings
   set forticlient-key-enforce enable
   set forticlient-reg-key <password>
end
```

FortiClient users can select to remember the connection key password in the FortiClient console when they connect FortiClient Telemetry.

Monitor FortiClient endpoints

You can monitor FortiClient endpoints in the FortiGate GUI. On FortiGate, each new connection is automatically added to the device table.

To view connected devices, go to *Monitor* > *FortiClient Monitor*.

Configure FortiClient Telemetry connections with AD user groups

When FortiClient Telemetry connects to FortiGate or EMS, the user's AD domain name and group are both sent to FortiGate or EMS. Administrators may configure the FortiGate or EMS to deploy endpoint and/or firewall profiles based on the end user's AD domain group.

The following steps are discussed in more details:

- Configure users and groups on AD servers
- Configure FortiAuthenticator
- Configure FortiGate or EMS
- Connect FortiClient Telemetry to FortiGate or EMS
- Monitor FortiClient connections

Configure users and groups on AD servers

Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time.

Configure FortiAuthenticator

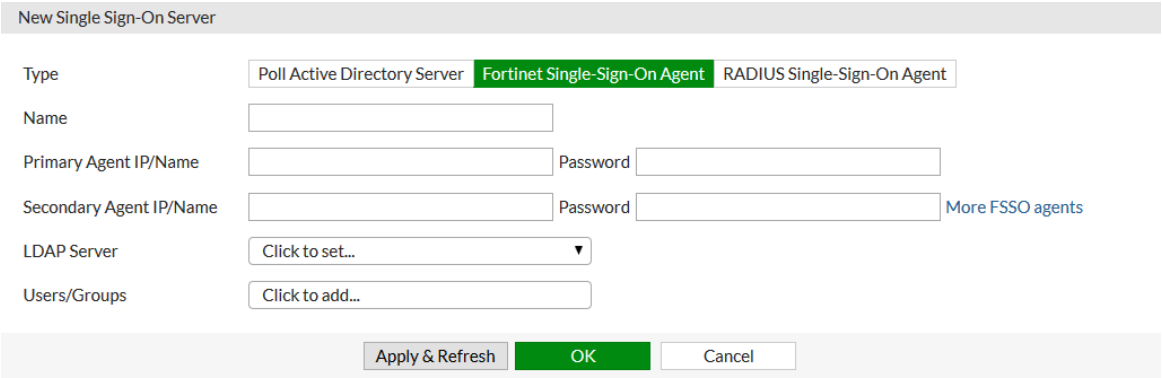
Configure FortiAuthenticator to use the AD server that you created. For more information see the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

Configure FortiGate or EMS

FortiGate

Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO):

1. Go to *User & Device* > *Single Sign-On*.
2. Select *Create New* in the toolbar. The *New Single Sign-On Server* window opens.



3. In the type field, select *Fortinet Single-Sign-On Agent*.
4. Enter the information required for the agent. This includes the name, primary and secondary IP addresses, and passwords. Select an LDAP server in the drop-down list if applicable. Select *More FSSO agents* to add up to three additional agents.
5. Select *OK* to save the agent configuration.

Create a user group:

1. Go to *User & Device* > *User Groups*.
2. Select *Create New* in the toolbar. The *New User Group* window opens.
3. In the type field, select *Fortinet Single-Sign-On (FSSO)*.
4. Select members from the drop-down list.
5. Select *OK* to save the group configuration.

Configure the FortiClient profile:

1. Go to *Security Profiles* > *FortiClient Profiles*.
2. Select *Create New* in the toolbar. The *New FortiClient Profile* window opens.
3. Enter a profile name and optional comments.
4. In the *Assign Profile To* drop-down list select the FSSO user group(s).
5. Configure FortiClient configuration as required.
6. Select *OK* to save the new FortiClient profile.

Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who connect successfully, but have no matching FortiClient profile.

Configure the firewall policy:

Configure the firewall policy as described in Configure firewall policies on page 35. Ensure that *Compliant with FortiClient Profile* is selected in the policy.

EMS

Add a new domain:

1. Under the *Endpoints* heading, in the *Domains* section, select *Add a new domain*. The *Domain Settings* window opens.
2. Enter the domain information as required.
3. Select *Test* to confirm functionality, then, if successful, select *Save* to add the domain.

The domain's organizational units (OUs) will automatically be populated in the *Domains* section under the *Endpoints* heading. For more information, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

Connect FortiClient Telemetry to FortiGate or EMS

The Microsoft Windows system on which FortiClient is installed should join the domain of the AD server configured earlier. Users may log in with their domain user name.

Following this, FortiClient endpoint connections will send the logged-in user's name and domain to the FortiGate or EMS. The FortiGate or EMS will assign the appropriate profiles based on the configurations.

Monitor FortiClient connections

The following FortiOS CLI command lists information about connected clients. This includes domain-related details for the client (if any).

```
diagnose endpoint record-list
   Record #1:
      IP_Address = 172.172.172.111(1)
      MAC_Address = b0:ac:6f:70:e0:a0
      Host MAC_Address = b0:ac:6f:70:e0:a0
      MAC list = b0-ac-6f-70-e0-a0;
      VDOM = root
      Registration status: Forticlient installed but not registered
      Online status: offline
      DHCP on-net status: off-net
      DHCP server: None
      FCC connection handle: 6
      FortiClient version: 5.1.29
      AVDB version: 22.137
      FortiClient app signature version: 3.0
      FortiClient vulnerability scan engine version: 1.258
      FortiClient feature version status: 0
      FortiClient UID: BE6B76C509DB4CF3A8CB942AED2064A0 (0)
      FortiClient config dirty: 1:1:1
      FortiClient KA interval dirty: 0
      FortiClient Full KA interval dirty: 0
      FortiClient server config: d9f86534f03fbed109676ee49f6cfc09::
      FortiClient config: 1
      FortiClient iOS server mconf:
      FortiClient iOS mconf:
      FortiClient iOS server ipsec_vpn mconf:
      FortiClient iOS ipsec_vpn mconf:
      Endpoint Profile: Documentation
      Reg record pos: 0
```

```
Auth_AD_groups:
Auth_group:
Auth_user:
Host_Name:
OS_Version: Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601)
Host_Description: AT/AT COMPATIBLE
Domain:
Last_Login_User: FortiClient_User_Name
Host_Model: Studio 1558
Host_Manufacturer: Dell Inc.
CPU_Model: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz
Memory_Size: 6144
Installed features: 55
Enabled features: 21
online records: 0; offline records: 1
status -- none: 0; uninstalled: 0; unregistered: 1; registered: 0; blocked: 0
```

FortiClient Provisioning

FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems by using Microsoft Active Directory (AD).

You can use FortiClient EMS to deply FortiClient to multiple Microsoft Windows systems. For information, see the *FortiClient EMS Administration Guide*.

This chapter contains the following sections:

- Install FortiClient on computers
- Install FortiClient on infected systems
- Install FortiClient as part of cloned disk images
- Deploy FortiClient using Microsoft Active Directory servers

For information on customizing your FortiClient installation, see Custom FortiClient Installations.

Download FortiClient installation files

The FortiClient installation files can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

  Requires a support account with a valid support contract. Download either the Microsoft Windows (32-bit/64-bit) or the Mac OS X installation file.

- FortiClient homepage: www.forticlient.com

  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

- Fortinet Resource Center: http://www.fortinet.com/resource_center/product_downloads.html

  Download the FortiClient online installation file. On this page you can download the latest version of FortiClient for Microsoft Windows and Mac OS X, and link to the iOS, and Android versions.

Install FortiClient on computers

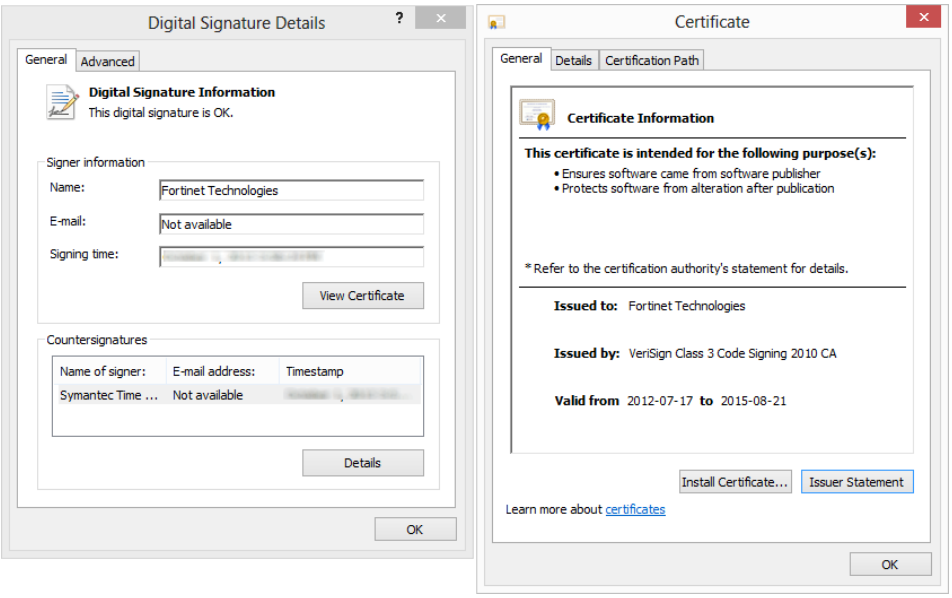
The following section describes how to install FortiClient on a computer that is running a Microsoft Windows or Apple Mac operating system.

Microsoft Windows computer

The following instructions will guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) Release Notes*.

When installing FortiClient, it is recommended to use the FortiClientOnlineInstaller file. This file will launch the FortiClient Virus Cleaner which will scan the target system prior to installing the FortiClient application.

To check the digital signature of FortiClient, right-click on the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.

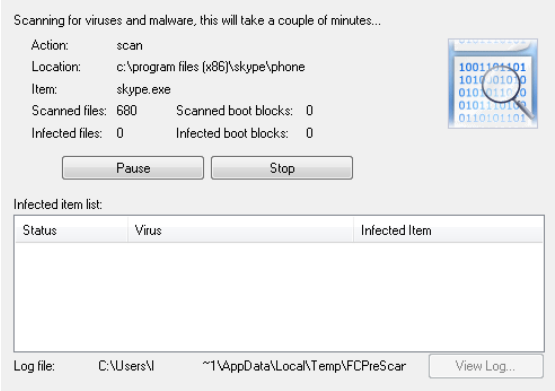


To install FortiClient (Windows):

1. Double-click the FortiClient executable file. The *Setup Wizard* launches.

   When using the FortiClient Online Installer file, the FortiClient Virus Cleaner will run before launching the *Setup Wizard*.

   If a virus is found that prevents the infected system from downloading the new FortiClient package, see Install FortiClient on infected systems on page 45.



2. In the *Welcome* screen, read the license agreement, select the *Yes, I have read and accept the license* checkbox, and select *Next* to continue. The *Choose Setup Type* screen is displayed.

   You can read the license agreement by clicking the *License Agreement* button. You have the option to print the EULA in this *License Agreement* screen.

3. Select one of the following setup types:
   - Complete: All Endpoint Security and VPN components will be installed.
   - VPN Only: Only VPN components (IPsec and SSL) will be installed.

4. Select *Next* to continue. The *Destination Folder* screen is displayed.
5. Select *Change* to choose an alternate folder destination for installation.
6. Select *Next* to continue.

   FortiClient will search the target system for other installed antivirus software. If found, FortiClient will display the *Conflicting Antivirus Software* page. You can either exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient real-time protection disabled.

This dialog box is displayed during a new installation of FortiClient and when upgrading from an older version of FortiClient, which does not have the antivirus feature installed.

It is recommended to uninstall the conflicting antivirus software before installing FortiClient or enabling the antivirus real-time protection feature. Alternatively, you can disable the antivirus feature of the conflicting software.

7. Select *Next* to continue.
8. Select *Install* to begin the installation.
9. Select *Finish* to exit the FortiClient Setup Wizard.

   On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now, or select *No* to manually restart later.

   FortiClient will update signatures and components from the FortiGuard Distribution Network (FDN).

10. FortiClient will attempt to connect FortiClient Telemetry to the FortiGate.

    If the FortiGate cannot be located on the network, manually connect FortiClient Telemetry. See Connect FortiClient Telemetry manually on page 52.

If you have any questions about connecting FortiClient Telemetry to FortiGate, please contact your network administrator.

11. To launch FortiClient, double-click the desktop shortcut icon.

Microsoft Server

You can install FortiClient on a Microsoft Windows Server 2008 R2, 2012, or 2012 R2 server. You can use the regular FortiClient Windows image for Server installations.

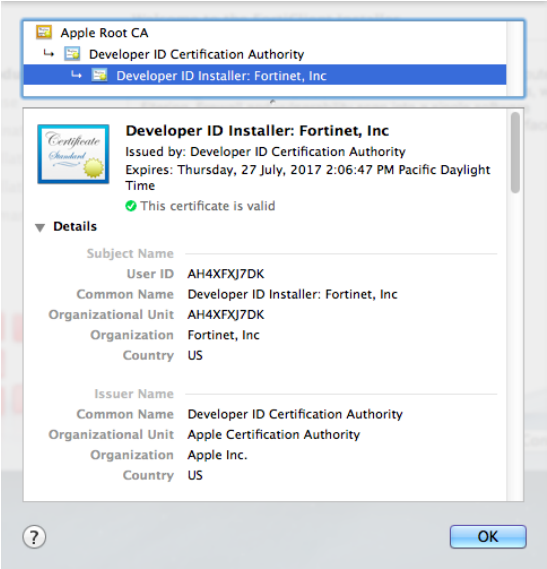
Please refer to the Microsoft knowledge base for caveats on installing antivirus software in a server environment. See the Microsoft Anti-Virus exclusion list: http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx

Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the *FortiClient (Mac OS X) Release Notes*.

To install FortiClient (Mac OS X):

1. Double-click the FortiClient `.dmg` installer file to launch the FortiClient installer. The *FortiClient Installer* will install FortiClient on your computer. Select *Continue*.
2. Select the lock icon in the upper right corner to view certificate details.



3. Read the Software License Agreement and select *Continue*. You have the option to print or save the Software Agreement in this window. You will be prompted to *Agree* with the terms of the license agreement.
4. Select the destination folder for the installation.
5. Select *Install* to perform a standard installation on this computer. You can change the install location from this screen.
6. Depending on your system, you may be prompted to enter your system password.
7. After the installation completes successfully, select *Close* to exit the installer.
8. FortiClient has been saved to the *Applications* folder.
9. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon in the FortiClient console to make changes to the FortiClient configuration.

Install FortiClient on infected systems

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading of the new FortiClient package, use the following process:

- Boot into “safe mode with networking” (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network).
- Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs sub-directory. If a virus is found, it will be quarantined. When complete, reboot back into normal mode and run the FortiClient installer to complete the installation.

Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message will be generated. It is necessary to reboot back into normal mode to complete the installation.

Install FortiClient as part of cloned disk images

If you configure computers using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image:

1. Install and configure the FortiClient application to suit your requirements.
   You can use a standard or a customized installation package.
2. Right-click the FortiClient icon in the system tray and select *Shutdown FortiClient*.
3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

   Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

   Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on.

5. Create the hard disk image and deploy it as needed.

Deploy FortiClient using Microsoft Active Directory servers

There are multiple ways to deploy FortiClient to endpoint devices including using Microsoft Active Directory (AD).

The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new Organizational Unit (OU).
7. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
8. Select *Start* > *Administrative Tools* > *Group Policy Management*t. The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and Link it here. Give the new GPO a name then select *OK*.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in will open.
10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
11. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package will then be generated.
12. If you wish to expedite the installation process, on both the server and client computers, force a GPO update.
13. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstall FortiClient using Microsoft Active Directory server:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* will open.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package that was used to install FortiClient.
3. Right-click the package, select *All Tasks* > *Remove*. Choose Immediately uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package will delete.
4. If you wish to expedite the uninstall process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Deploy FortiClient using EMS

You can use FortiClient EMS to deploy FortiClient (Windows) in managed mode to devices in your network that are running a supported Windows operating system. For installation information, see the FortiClient

EMS Administration Guide.

An upgrade schedule dialog box is displayed in advance when deploying FortiClient from EMS to endpoints running Windows operating system. If no FortiClient is installed on the endpoint, no reboot is required for the installation, and no upgrade schedule dialog box is displayed. The user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog box is displayed with a 15 minute warning.

Upgrade FortiClient

For information about supported upgrade paths for FortiClient, see the *FortiClient Release Notes*.

FortiClient Telemetry Connection

The section applies only to FortiClient in managed mode.

In managed mode, FortiClient uses a gateway IP address to connect FortiClient Telemetry to FortiGate or FortiClient EMS. For more information, see Telemetry Gateway IP Lists on page 31.

How FortiClient locates FortiGate or EMS

FortiClient uses the following methods in the following order to locate FortiGate or EMS for Telemetry connection:

- Manual entering of the gateway IP address, which means that the endpoint user enters the gateway IP address of FortiGate or EMS into FortiClient console. See Connect FortiClient Telemetry manually on page 52.
- Telemetry Gateway IP list

  FortiClient Telemetry searches for IP addresses in its subnet in the Gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system.

  If FortiClient cannot find any FortiGates in its subnet, it will attempt to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the Gateway IP list.
- Default gateway IP address

  The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connection to EMS.

FortiClient obtains the default gateway IP address from the operating system on the endpoint device. The default gateway IP address of the endpoint device should be the IP address for the FortiGate interface with Telemetry enabled.

- VPN
- Remembered gateway IP list

  You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate or EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate or EMS.

FortiClient uses the same process to connect Telemetry to FortiGate or EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

Connect FortiClient Telemetry after installation

After FortiClient software installation completes on an endpoint, FortiClient automatically launches and searches for a FortiGate or FortiClient EMS for FortiClient Telemetry connection. See also How FortiClient locates FortiGate or EMS on page 49.

When FortiClient locates a FortiGate or EMS, the *FortiGate Detected* or *Enterprise Management Server (EMS) Detected* dialog box is displayed.

The following options are availble:

Endpoint User	Displays the name of the endpoint user that is logged into the endpoint device.
Logged into Domain	Displays the name of domain if applicable.
Hostname	Displays the name of the endpoint device.
Profile Details	Click to display details of the profile that FortiClient will download after you accept connection to FortiGate or EMS. See also FortiClient profiles on page 26.
Remember this FortiGate	Select for FortiClient to remember the gateway IP address of the FortiGate or EMS to which you are connecting Telemetry. See also Remember gateway IP addresses on page 50.

Click *Accept* to connect FortiClient Telemetry to the identified FortiGate or EMS. Alternately, you can click *Cancel* to launch FortiClient software without connecting FortiClient Telemetry. FortiClient launches in standalone mode. You can manually connect FortiClient Telemetry later.

After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient downloads a profile from FortiGate or EMS. A system tray bubble message will be displayed once the profile download is complete.

Remember gateway IP addresses

When you confirm Telemetry connection to a FortiGate or EMS, you can instruct FortiClient to remember the gateway IP address of the FortiGate or EMS. If a connection key is required, FortiClient remembers the connection password too. FortiClient can remember up to 20 gateway IP addresses for FortiGate and EMS.

The remembered IP addresses display in the Local Gateway IP list. FortiClient can use the remembered gateway IP addresses to automatically connect to FortiGate or EMS.

See also Forget gateway IP addresses on page 58.

To remember IP addresses for FortiGate or EMS:

1. In the *FortiGate or EMS Detected* dialog box, select the *Remember this FortiGate* or *Remember this EMS* (not shown) check box.

2. Click *Accept*.
   FortiClient remembers the IP address and password, if applicable.

Compliance

The *Compliance* tab displays whether FortiClient Telemetry is connected to FortiGate or EMS.

When FortiClient Telemetry is connected to FortiGate, the *Compliance* tab displays whether FortiClient and the endpoint device are compliant with the compliance rules defined by FortiGate. When FortiClient and/or the endpoint device are not compliant, the *Compliance* tab displays information about how FortiClient and the endpoint device can be returned to a status of compliant.

You can also use the *Compliance* tab to connect FortiClient Telemetry to FortiGate or EMS and disconnect FortiClient Telemetry from FortiGate or EMS.

Enable compliance

For FortiClient in standalone mode, the *Compliance* tab is not used.

For FortiClient in managed mode, an administrator enables and disables endpoint compliance by using FortiGate. When endpoint compliance is enabled, FortiClient must be installed on endpoint devices, and FortiClient Telemetry must be connected to FortiGate. When FortiClient Telemetry is connected, the FortiClient endpoint receives a profile from FortiGate that contains the compliance rules and optionally some FortiClient configuration information.

If FortiGate is integrated with EMS, the FortiClient endpoint might also receive a profile from EMS that contains FortiClient configuration information.

Connect FortiClient Telemetry manually

On endpoints, FortiClient Telemetry can be connected using one of the following options:

- FortiGate
- EMS
- FortiGate and EMS

If FortiClient Telemetry was not automatically connected after FortiClient installation, you can manually connect FortiClient Telemetry to FortiGate or EMS.

To manually connect FortiClient Telemetry to FortiGate:

1. Go to the *Compliance* tab.
2. In the *FortiGate IP* box, type the IP address or URL of FortiGate, and click *Connect*.

   FortiClient Telemetry connects to FortiGate, and FortiClient downloads a profile of compliance rules from FortiGate.

To manually connect FortiClient Telemetry to EMS:

1. Go to the *Compliance* tab.
2. In the *FortiGate IP* box, type the IP address or URL of EMS, and click *Connect*.

FortiClient Telemetry connects to EMS, and FortiClient downloads a profile of configuration information from EMS.

To manually connect FortiClient Telemetry to FortiGate and EMS:

1. Go to the *Compliance* tab.
2. In the *FortiGate IP* box, type the IP address or URL of FortiGate, and click *Connect*.

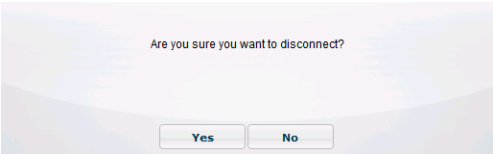
   FortiClient Telemetry establishes the primary connection to FortiGate, and FortiClient downloads a profile of compliance rules from FortiGate. FortiClient Telemetry automatically also establishes a secondary connection to EMS, and FortiClient downloads a profile of configuration information from EMS.

Disconnect FortiClient Telemetry

You must disconnect FortiClient Telemetry from FortiGate or EMS to connect to another FortiGate or EMS or to uninstall FortiClient.

To disconnect FortiClient Telemetry:

1. On the *Compliance* tab, click the *Click to Disconnect* link. A confirmation dialog box is displayed.



2. Click *Yes* to disconnect FortiClient from FortiGate or EMS.

After you disconnect FortiClient Telemetry from FortiGate or EMS, FortiClient Telemetry automatically connects with the FortiGate or EMS when you re-join the network. See also Forget gateway IP addresses on page 58.

View compliance status

Information available on the *Compliance* tab depends on whether FortiClient is running in standalone mode or managed mode. In managed mode, the information displayed on the *Compliance* tab also depends on whether FortiClient Telemetry is connected to FortiGate or FortiClient EMS.

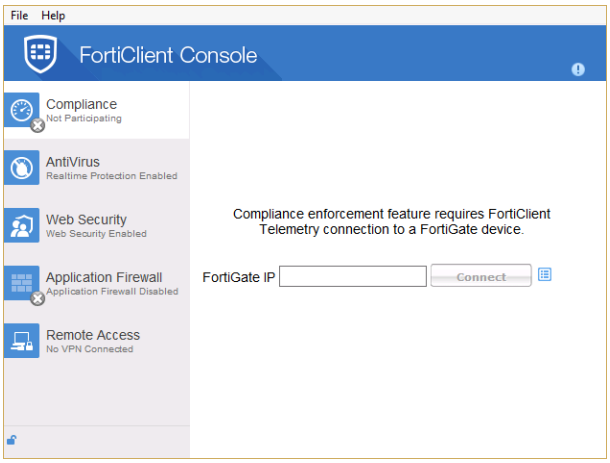
When FortiClient Telemetry is connected to EMS and the feature is enabled in EMS, a picture of the endpoint user might display on the *Compliance* tab. FortiClient displays the picture that is defined for the Windows operating system on the endpoint device. If FortiClient cannot find a picture defined for the Windows operating system on the endpoint device, no picture is displayed on the *Compliance* tab.

Standalone mode

When FortiClient is running in standalone mode, the *Compliance* tab is not used. The *Compliance* tab is labeled *Not Participating*. The unlocked icon at the bottom left of the screen indicates that settings in FortiClient console

are unlocked, and the endpoint user can change them.

If you want to use the compliance feature, you must connect FortiClient Telemetry to FortiGate.

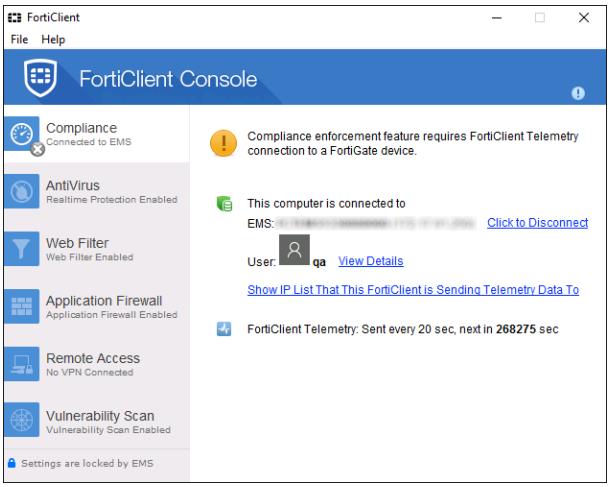


The *Compliance* tab displays the following information:

FortiGate IP	Type the IP address or URL of FortiGate or EMS, and click *Connect* to connect FortiClient Telemetry.
Unlocked icon	Indicates that the settings in FortiClient console are unlocked and can be changed.

FortiClient Telemetry connected to EMS

When FortiClient Telemetry is connected to EMS, compliance is not enforced. The *Compliance* tab is labeled *Connected to EMS*. The locked icon at the bottom left of the screen indicates that settings in the FortiClient console are locked by EMS. EMS controls the settings by pushing a profile to FortiClient.



The *Compliance* tab displays the following information:

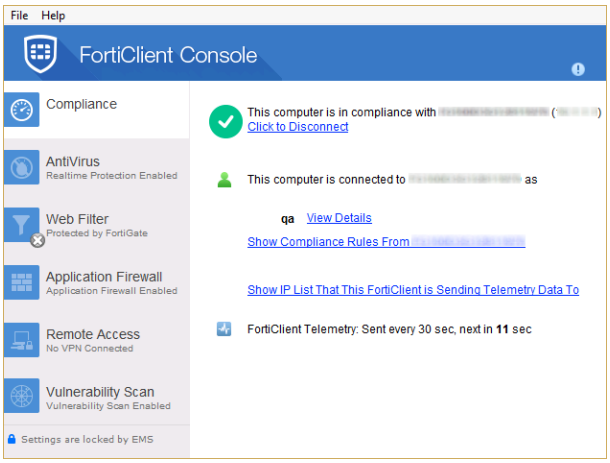
Compliance status	Indicates that the compliance enforcement feature requires FortiClient Telemetry connection to FortiGate.
FortiClient EMS information	Displays the name and IP address of the EMS to which FortiClient Telemetry is connected. You can disconnect by clicking the *Click to Disconnect* link, view details about the endpoint device by clicking the *View Details* link, and view the gateway IP list that FortiClient is using for FortiClient Telemetry connection by clicking the *Show IP List That This FortiClient is Sending Telemetry Data to* link.
FortiClient Telemetry information	Displays how often FortiClient Telemetry communicates with FortiClient EMS and when the next communication will occur. FortiClient Telemetry also downloads FortiClient configuration information from EMS.
Locked icon	Indicates that the settings in FortiClient console are locked by EMS.

FortiClient Telemetry connected to FortiGate

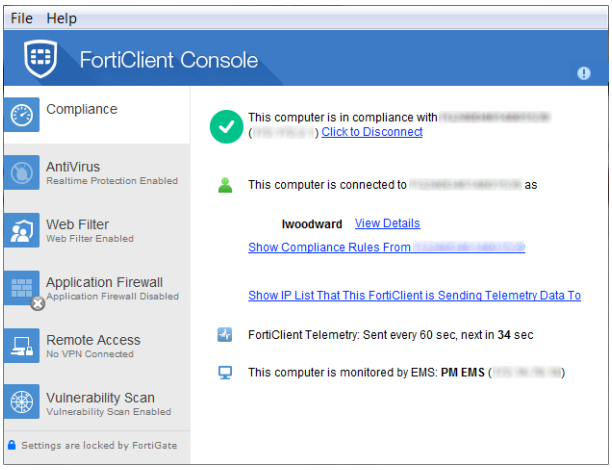
When FortiClient Telemetry is connected to FortiGate, network access compliance is enforced. The locked icon at the bottom left of the screen indicates one of the following statuses:

- The settings in the FortiClient console are locked by the profile from EMS. In this case, FortiGate is integrated with EMS, and the non-compliance action in FortiGate is set to block or warn. FortiGate provides the compliance rules, and EMS provides the profile of FortiClient settings.
- The settings in the FortiClient console are unlocked. In this case, FortiGate provides the compliance rules, and the non-compliance action in FortiGate is set to auto-update. You can change the FortiClient settings unrelated to the compliance rules.

In the following example, FortiClient Telemetry is connected to FortiGate, but EMS provides the profile of FortiClient settings. The settings are locked by EMS.



In the following example, FortiClient Telemetry is connected to FortiGate, and a profile is not provided by EMS. The settings are locked by FortiGate.



The *Compliance* tab displays the following information:

Compliance status	Displays the compliance status of the computer on which FortiClient is installed. The computer is either in compliance or not compliant with FortiGate.
FortiGate information	Displays the name and IP address of the FortiGate to which FortiClient Telemetry is connected. You can perform the following actions: • Disconnect FortiClient Telemetry by clicking the *Click to Disconnect* link • View details about the endpoint device by clicking the *View Details* link • View compliance rules from FortiGate by clicking the *Show Compliance Rules From <FortiGate>* link • View the gateway IP list being used for FortiClient Telemetry connection by clicking the *Show IP List That This FortiClient is Sending Telemetry Data to* link.
FortiClient Telemetry information	Displays how often FortiClient Telemetry communicates with FortiGate and when the next communication will occur. FortiClient Telemetry communicates information between FortiClient and FortiGate, sending status information to FortiGate and receiving network-access rules and possibly some FortiClient configuration information from FortiGate. When FortiGate is integrated with EMS, notification information is also sent to EMS. Depending on the FortiGate settings, EMS might also send FortiClient configuration information to FortiClient.
Monitoring	Displays whether the endpoint is managed by EMS.
Locked or unlocked icon	Indicates whether the settings in FortiClient console are unlocked or locked by FortiGate or EMS.

View user details

You can view user details when FortiClient is compliant with FortiGate rules. You cannot view user details when FortiClient is not compliant with FortiGate rules.

To view user details:

1. On the *Compliance* tab, view the name of the user beside the *View Details* link.
2. Click the *View Details* link to view the following information:

Online/offline	Displays whether the endpoint device is online or offline. A green icon indicates the endpoint is online.
Off-Net/On-Net	Displays whether the endpoint device is on-net or off-net. A green *On-Net* icon indicates the endpoint is on-net.
Username	Displays the name of the user logged into FortiClient on the endpoint.
Hostname	Displays the name of the device on which FortiClient is installed.
Domain	Displays the name of the domain to which the endpoint device is connected, if applicable.

3. Click the *X* to close the dialog box.

View gateway IP lists

You can view the following gateway IP lists in FortiClient:

- Gateway IP List

  The Gateway IP list is created by administrators. Endpoint users cannot change the list. For more information, see Telemetry Gateway IP Lists on page 31.

- Local Gateway IP List

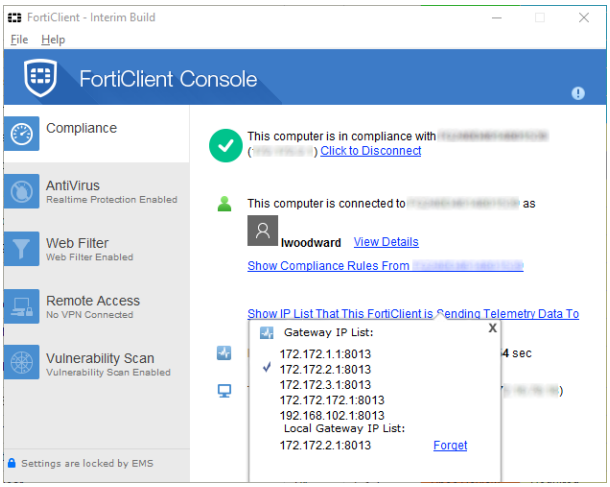
  The Local Gateway IP list is created by endpoint users. It is the list of remembered FortiGate or EMS devices. When FortiClient Telemetry is connected for the first time, you can choose to remember the gateway IP address. See Remember gateway IP addresses on page 50.

The gateway IP lists are used to automatically connect FortiClient Telemetry to FortiGate or EMS.

To view gateway IP lists:

1. On the *Compliance* tab, click the *Show IP List That This FortiClient is Sending Telemetry Data to* link.

   The Gateway IP List and the Local Gateway IP List are displayed.



2. Click *X* to close the list.

Forget gateway IP addresses

When you instruct FortiClient to forget an IP address for FortiGate or EMS, FortiClient Telemetry will not use the IP address to automatically connect to FortiGate or EMS when re-joining the network.

To forget FortiGate or EMS:

1. On the *Compliance* tab, click the *Show IP List That This FortiClient is Sending Telemetry Data to* link.
2. In the *Local Gateway IP List*, click *Forget* beside the gateway IP addresses that you no longer want FortiClient to remember.
3. Click *X* to close the list.

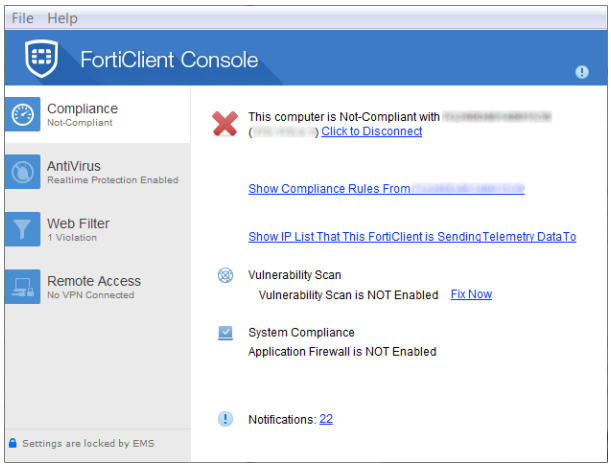
Fix not compliant status

You can maintain compliance by ensuring that FortiClient software is configured to meet the requirements specified in the compliance rules defined by the FortiGate to which FortiClient Telemetry is connected. FortiGate might also require the endpoint device to run a specific version of FortiClient or operating system software.

When FortiClient displays a status of Not-Compliant, you can take actions that will make FortiClient compliant with FortiGate again.

View not-compliant status

When a FortiClient endpoint does not comply with the FortiGate compliance rules, the *Compliance* tab displays a status of *Not-Compliant*.



The following information is displayed on the *Compliance* tab:

This computer is Not Compliant with	Displays the name and IP address of the FortiGate to which FortiClient Telemetry is connected. You can view the compliance rules by clicking the *Show Compliance Rules from <FortiGate>* link.
Vulnerability Scan	Displays critical vulnerabilities found for the endpoint when detected. You must fix the critical vulnerabilities to return to compliant status by clicking *Fix Now*. You can also click the *Details* link to view details about the vulnerabilities. In some cases, you must manually update software that is running on the device within a specified time frame to remain compliant.
Software Out of Date	Displays whether FortiClient software is outdated. You must upgrade to the specified FortiClient version to return to compliant status by clicking *Update Now*.
System Compliant	Displays whether the operating system of the endpoint complies with FortiGate rules. You must use the specified operating system to return to compliant status. You can view the allowed operating systems by clicking the *Details* link.
Fix All	Click to fix all reported issues. This option is available when the non-compliance setting in FortiGate is set to block or warn, and EMS has not provided a profile to the FortiClient endpoint. This option is not available when the non-compliance setting in FortiGate is set to auto-update. If the *Fix All* link is not displayed, contact your administrator to help adjust the FortiClient Console and computer settings to remain in compliance with FortiGate.

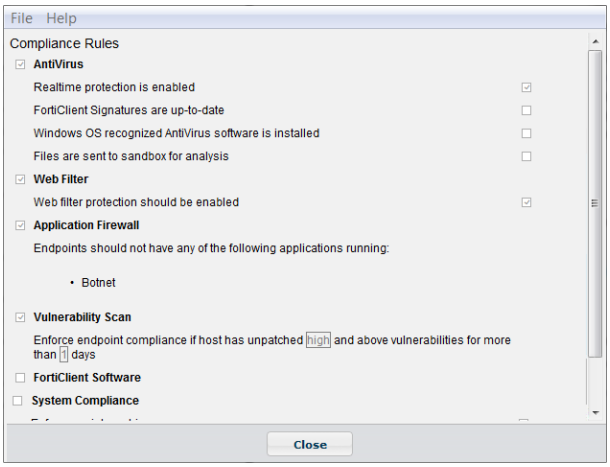
View compliance rules

When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the settings required on FortiClient console for the FortiClient endpoint to remain compliant.

You cannot view compliance rules when FortiClient Telemetry is connected to EMS.

To view compliance rules:

1. On the *Compliance* tab, click the *Show Compliance Rules From <FortiGate>* link.
   The compliance rules from FortiGate are displayed.



2. Click *Close* to return to the *Compliance* tab.

Fix now

Issues that caused a not-compliant status can be fixed to return FortiClient endpoints to a compliant status. When available, you can click the *Update Now*, *Fix Now*, or *Fix All* links on the *Compliance* tab to return FortiClient endpoints to compliant status.

When FortiClient has a not compliant status and the Update Now, Fix Now, or Fix All links are not displayed, endpoint users should contact their system administrator for help with configuring the endpoint and FortiClient Console to remain in compliance with FortiGate.

What links are available depend on the configuration of FortiGate and EMS. The following table summarizes when links are available:

Configuration	Compliance Rules	FortiClient Configuration	Options
FortiGate	Yes	No	FortiClient settings are unlocked. Click *Update Now*, *Fix Now*, and *Fix All* links when available.

Configuration	Compliance Rules	FortiClient Configuration	Options
FortiGate integrated with EMS	Yes	No	FortiClient settings are unlocked. Click *Update Now*, *Fix Now*, and *Fix All* links when available.
	Yes	Yes	FortiClient settings are locked by EMS. Use EMS to update the profile that contains the FortiClient configuration to meet the requirements of the compliance rules.

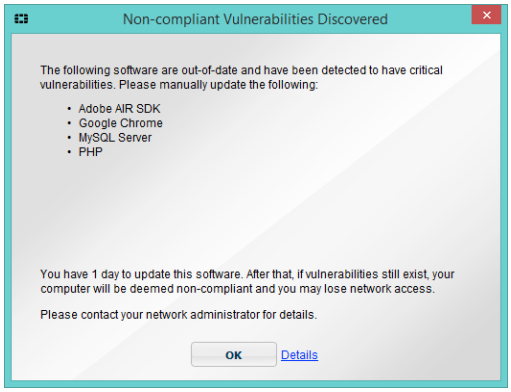
To fix now:

1. On the *Compliance* tab, perform one of the following options:
   - Click *Fix All*.
   - Click *Update Now*.
   - Click *Fix Now*.

   The non-compliance issues are fixed, and the FortiClient endpoint returns to a status of compliant.
2. If the *Fix All*, *Update Now*, or *Fix Now* links are not displayed on the Compliance tab, contact your system administrator for help with changing the endpoint and FortiClient Console settings.

Manually fix software vulnerabilities

In some cases, you must manually install software updates to maintain compliance. When your action is required to address software vulnerabilities, FortiClient displays a dialog box that informs you what software you must update and how long you have to update the software. Following is an example of the dialog box.



If you fail to update the identified software within the specified time frame, the status of FortiClient changes to Not-Compliant, and you may lose access to the network. If you lose access to the network, contact your system administrator for assistance.

Examples of blocked FortiClient endpoints

FortiClient endpoint access to the network can be blocked a number of ways. The following table provides examples of how FortiClient endpoints can be blocked from accessing the network and how to regain access.

Configuration	Failure	Blocked By	Solution
Endpoint control is enabled on FortiGate. FortiClient Telemetry is connected to FortiGate.	FortiClient configuration fails to meet the compliance rules specified by FortiGate	FortiClient	View the *Compliance* tab in FortiClient console, and follow the instructions to configure FortiClient to meet the compliance rules specified by FortiGate.
Endpoint control is enabled on FortiGate. FortiClient Telemetry is not connected to FortiGate.	FortiClient Telemetry is not connected	FortiGate	In FortiClient console, connect FortiClient Telemetry to FortiGate.

View notifications

Select the notifications icon in the FortiClient console to view notifications. When a virus has been detected, the notifications icon will change from gray to yellow.

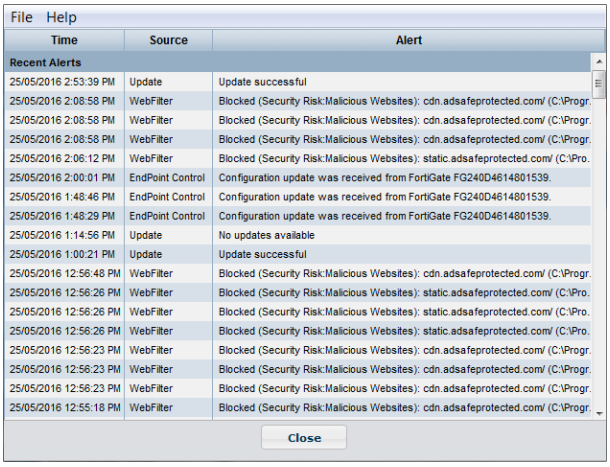
Event notifications include:

- Antivirus events including scheduled scans and detected malware.
- Endpoint Control events including configuration updates received from FortiGate.
- WebFilter events including blocked web site access attempts.
- System events including signature and engine updates and software upgrades.

Select the *Threat Detected* link to view quarantined files, site violations, and real-time protection events.

To view notifications:

1. In FortiClient Console, click the *Notifications* icon in the top-right corner.
   The list of notifications is displayed.



2. Click *Close* to close the list.

Antivirus

FortiClient includes an antivirus module to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient will also scan for and remove rootkits. In FortiClient, file-based malware, malicious websites, phishing, and spam URL protection are part of the antivirus module. Scanning can also be extended by using FortiSandbox.

Enable/disable realtime protection

For FortiClient in standalone mode, you can enable and disable realtime protection by using the FortiClient console.

For FortiClient in managed mode, an administrator enables, disables, and configures realtime protection by using a FortiClient profile. See FortiClient profiles on page 26.

Enable/disable Antivirus

This setting can only be configured when FortiClient is in standalone mode.

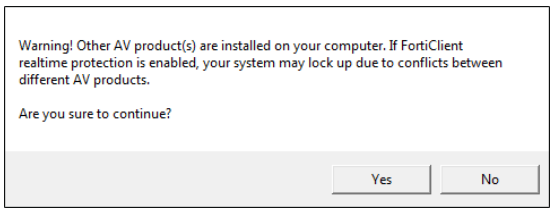
To enable Antivirus:

1. On the *AntiVirus* tab, click the settings icon next to *Realtime Protection Disabled*. The real-time protection settings page opens.
2. Select the *Scan files as they are downloaded or copied to my system* check box.
3. Click *OK*.

If you have another antivirus program installed on your system, FortiClient will show a warning that your system may lock up due to conflicts between different antivirus products.

Conflicting antivirus warning

It is recommended to remove the conflicting antivirus product before installing FortiClient or enabling the antivirus real-time protection feature.



To disable antivirus:

1. On the *AntiVirus* tab, click the settings icon next to *Realtime Protection Enable*. The real-time protection settings page opens.

2. Clear the *Scan files as they are downloaded or copied to my system* check box, and click *OK*.

Enable/disable FortiSandbox

This setting can only be configured when FortiClient is in standalone mode.

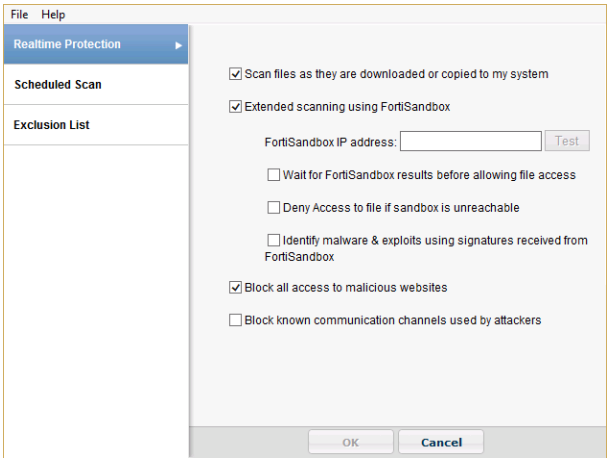
FortiClient integration with FortiSandbox allows you to submit files to FortiSandbox for automatic scanning. When configured, FortiClient will send supported files downloaded over the internet to FortiSandbox if they cannot be detected by the local, real-time scanning. Access to the downloaded file is blocked until the scanning result is returned.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all real-time and on-demand AV scanning.

You cannot configure this option when FortiClient is connected to FortiGate or EMS. The administrator configures this option on FortiGate or EMS.

To enable FortiSandbox:

1. On the *AntiVirus* tab, select the settings icon to open the real-time protection settings page.
2. Select *Extend scanning using FortiSandbox*.



3. Enter the FortiSandbox IP address, then select *Test* to ensure that the connection is correct.

4. Set the remaining options as needed.
5. Click *OK* to apply your changes.

Block access and communication channels

This setting can only be configured when FortiClient is in standalone mode.

To block access and communication channels:

1. On the *AntiVirus* tab, select the settings icon to open the real-time protection settings page.
2. Select *Block all access to malicious websites* and *Block known communication channels used by attackers*.
3. Click *OK* to apply your changes.

Enable/disable FortiSandbox scanning of files on removable media

This setting can be configured when FortiClient is in standalone or managed mode by using an XML configuration.

FortiSandbox can be enabled to scan files on removable media that are connected to endpoint devices. You must configure this option by using a FortiClient XML configuration. Realtime protection and FortiSandbox must be enabled before you can enable scanning of files on removable media.

FortiSandbox can scan files on the following types of removable media:

- USB drives
- Mapped drives

When enabled, FortiSandbox automatically scans files on removable media when you click a file. Alternately, you can manually send files on removable media to FortiSandbox for scanning

Scan and analysis on demand

You can perform on-demand antivirus scanning when FortiClient is in standalone or managed mode. You can scan specific files or folders, and you can submit a file for analysis.

Scan now

To perform on-demand antivirus scanning, select the *Scan Now* button in the FortiClient console. Use the drop-menu to select *Custom Scan*, *Full Scan*, *Quick Scan*, or *Removable media Scan*. The console displays the date of the last scan to the left of the button.

- *Custom Scan* runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
- *Full Scan* runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan including all files, executable files, DLLs, and drivers for threats.
- *Quick Scan* runs the rootkit detection engine to detect and remove rootkits. It only scans executable files, DLLs, and drivers that are currently running for threats.
- *Removable media Scan* runs the rootkit detection engine to detect and remove rootkits. It scans all connected removable media, such as USB drives.

Scan files or folders

To perform a virus scan a specific file or folder on your workstation, right-click the file or folder and select *Scan with FortiClient AntiVirus* from the menu.

Submit files for analysis

You can select to send up to 5 files a day to FortiGuard for analysis.

> You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files which are submitted for analysis and determined to be malicious.

To submit a file:

1. On your workstation, right-click a file or executable, and select *Submit for analysis* from the menu.
   A dialog box will be displayed which allows you to see the number of files you have submitted.
2. Confirm the location of the file you want to submit, and click the *Submit* button.

Scan with FortiSandbox on demand

You can send files to FortiSandox for scanning on demand when FortiClient is in managed mode and FortiSandbox is enabled.

To scan with FortiSandbox on demand:

1. Right-click a file and select *Scan with FortiSandbox* from the menu.

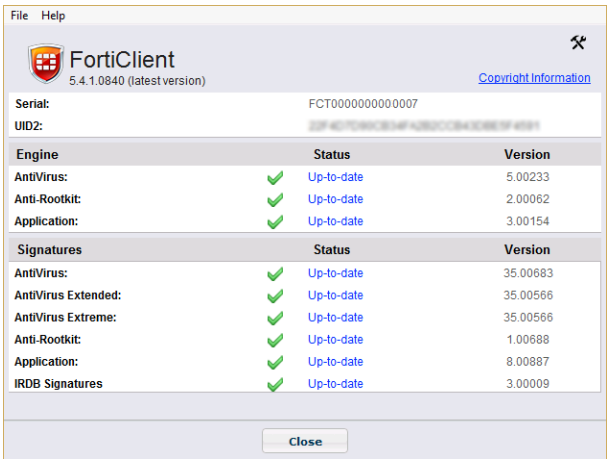
View FortiClient engine and signature versions

You can view the current FortiClient version, engine, and signature information when FortiClient is in standalone or managed mode.

> When FortiClient is connected to FortiGate for endpoint control, you can select to use a FortiManager device for client software and signature updates. When configuring the FortiClient profile, select *Use FortiManager for client software/signature updates* to enable the feature, and enter the IP address of your FortiManager device. You can select to failover to FDN when FortiManager is not available.

To view the current FortiClient version:

1. Go to *Help* > *About*.



2. Hover the mouse over the *Status* field to see the date and time that FortiClient last updated the selected item.
3. Click *Close*.

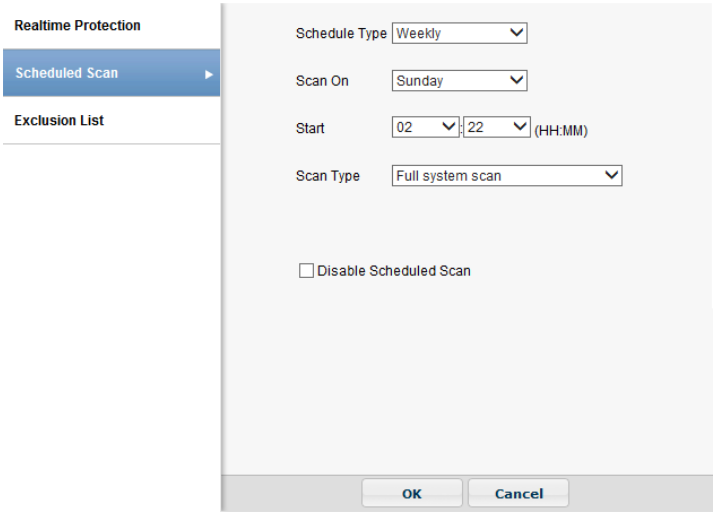
Schedule antivirus scanning

This setting can only be configured when FortiClient is in standalone mode.

If you configure monthly scans to occur on the 31st of each month, the scan will occur on the first day of the month for those months with less than 31 days.

To schedule antivirus scanning:

1. On the *AntiVirus* tab, click the *Settings* icon beside *Realtime Protection*.
2. Click the *Scheduled Scan* tab.



3. Configure the following settings:

Schedule Type	Select *Daily*, *Weekly*, or *Monthly* from the drop-down list.
Scan On	For Weekly scheduled scan, select the day of the week in the drop-down list. For Monthly scheduled scan, select the day of the month in the drop-down list.
Start	Select the time of day that the scan starts. The time format uses a 24-hour clock.
Scan Type	Select the scan type: • *Quick system scan* runs the rootkit detection engine to detect and remove rootkits. It only scans executable files, DLLs, drivers that are currently running for threats. • *Full system scan* runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan including all files, executable files, DLLs, and drivers for threats. • *Custom scan* runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. You cannot schedule a removable media scan. A full scan will scan removable media.
Disable Scheduled Scan	Select to disable scheduled scan.

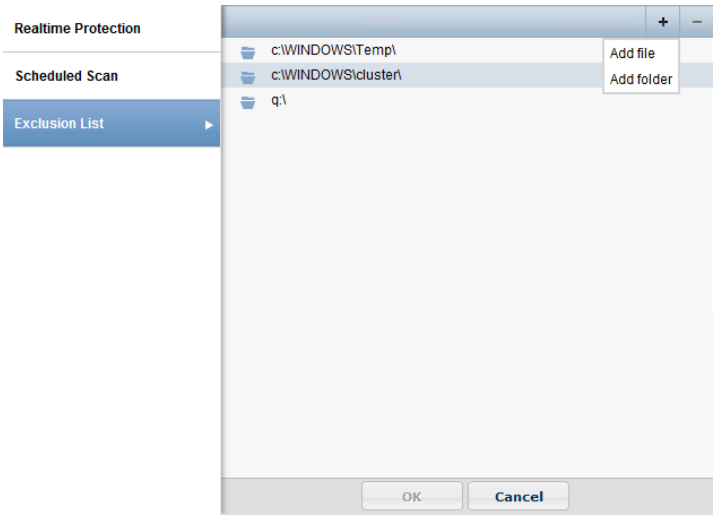
4. Click *OK* to save the setting and return to the main FortiClient console page.

Add files or folders to exclusion lists

This setting can only be configured when FortiClient is in standalone mode.

To add files/folders to the antivirus exclusion list:

1. On the *AntiVirus* tab, click the *Settings* icon beside *Realtime Protection*.
2. Click the *Exclusion List* tab.
3. Click the *Add* icon, and select *Add file* or *Add folder* from the drop-down list.
   Any files or folders in this exclusion list will not be scanned.



4. Click the *Minus* icon to remove files or folders from the list.
5. Click *OK* to save the setting and return to the FortiClient console page.

View scan results

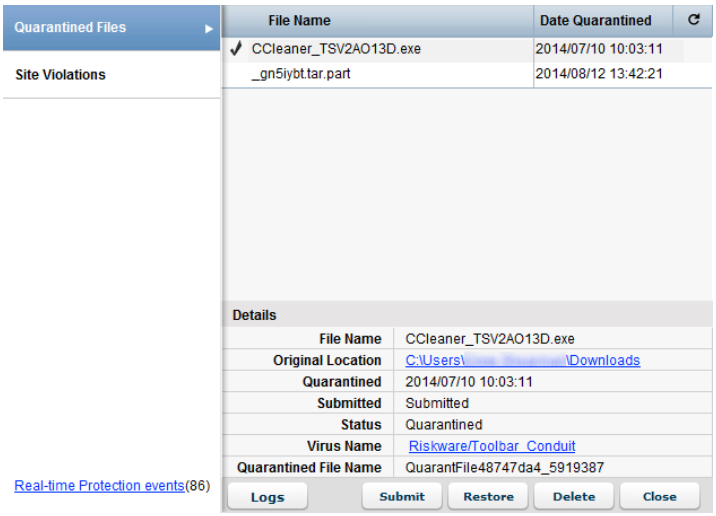
You can view quarantined threats, site violations, alerts, and realtime protection events when FortiClient is in standalone or managed mode.

View quarantined threats

To view quarantined threats:

1. On the *AntiVirus* tab, click the *X Threats Detected* link
2. Click the *Quarantined Files* tab.

   In this page you can view, restore, or delete the quarantined file. You can also view the original file location, the virus name, submit the suspicious file to FortiGuard, and view logs.



This page displays the following:

File Name	The name of the file.
Date Quarantined	The date and time that the file was quarantined by FortiClient.
Refresh	Select to refresh the quarantined files list.
Details	Select a file from the list to view detailed information including the file name, original location, date and time that the virus was quarantined, the submitted status, status, virus name, and quarantined file name.
Logs	Select to view FortiClient log data.
Refresh	Select to refresh the list.
Submit	Select to submit the quarantined file to FortiGuard. Press and hold the control key to submit multiple entries.
Restore	Select to restore the quarantined file. A confirmation dialog box will be displayed. You can select *Yes* to add this file/folder to the exclusion list, *No* to restore the file, or *Cancel* to exit the operation. Press and hold the control key to restore multiple entries.
Delete	Select to delete the quarantined file. A confirmation dialog box will be displayed, select *Yes* to continue. Press and hold the control key to delete multiple entries.
Close	Select to close the page and return to the FortiClient console.

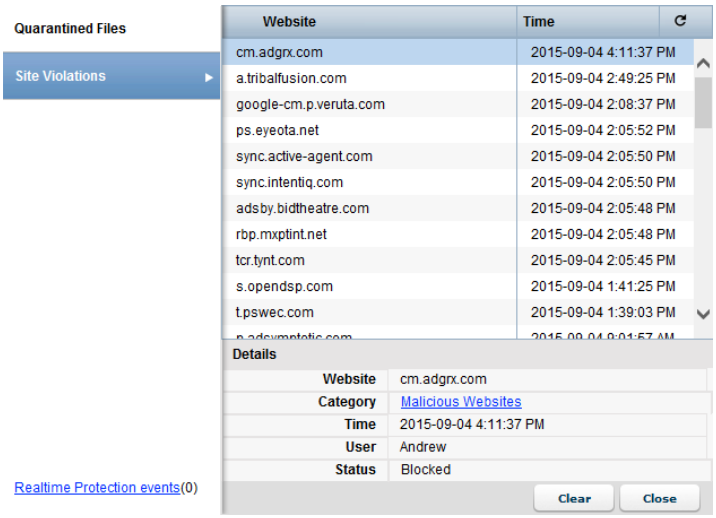
3. Click *Close*.

View site violations

On the *Site Violations* page, you can view site violations, and submit sites to be re-categorized.

To view site violations:

1. On the *AntiVirus* tab, click the *X Threats Detected* link.
2. Click the *Site Violations* tab.



This *Site Violations* page displays the following options:

Website	Displays the name of the website.
Time	Displays the date and time of the site violation.
Refresh	Select to refresh the site violation list.
Details	Select an entry in the list to view site violation details including the website name, category, date and time, user name, and status. Select the category link to request to have the site category re-evaluated.

3. Click *Close*.

View alerts

When FortiClient antivirus detects a virus while attempting to download a file via a web-browser, a warning displays in a dialog box.

Select *View recently detected virus(es)* to collapse the virus list. Right-click a file in the list to access the context menu.

Delete	Select to delete a quarantined or restored file.
Quarantine	Select to quarantine a restored file.
Restore	Select to restore a quarantined file.
Submit Suspicious File	Select to submit a file to FortiGuard as a suspicious file.

Submit as False Positive	Select to submit a quarantined file to FortiGuard as a false positive.
Add to Exclusion List	Select to add a restored file to the exclusion list. Any files in the exclusion list will not be scanned.
Open File Location	Select to open the file location on your workstation.

When *Alert when viruses are detected* under *AntiVirus Options* on the *Settings* page is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.

View realtime protection events

When an antivirus real-time protection event has occurred you can select to view these events in the FortiClient console. From the *AntiVirus* tab, select *X Threats Detected*, then select *Real-time Protection events (x)* in the left pane. The `realtime_scan.log` will open in the default viewer.

Example log output:

```
Realtime scan result:
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com.txt
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicarcom2.zip
time: 09/29/15 10:46:08, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar_com.zip
time: 09/29/15 10:46:39, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\3g_bl8y9.com.part
time: 03/18/15 10:48:13, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\xntwh8q1.zip.part
```

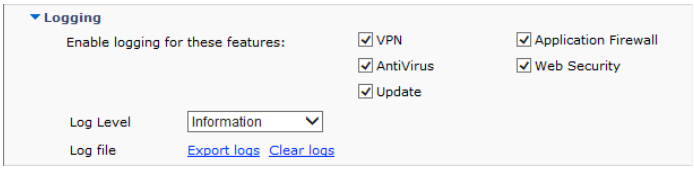
Configure Antivirus logging

In standalone mode, you can configure Antivirus logging by using the FortiClient console.

In managed mode, Antivirus logging is configured by using a FortiClient profile.

To configure Antivirus logging:

1. From the *File* menu, select *Settings*, and expand the *Logging* section.



2. Configure the following settings:

Enable logging for these features	Select antivirus to enable logging for this feature.
Log Level	Select the level of logging: • *Emergency*: The system becomes unstable. • *Alert*: Immediate action is required. • *Critical*: Functionality is affected. • *Error*: An error condition exists and functionality could be affected. • *Warning*: Functionality could be affected. • *Notice*: Information about normal events. • *Information*: General information about system operations. • *Debug*: Debug FortiClient.
Log file	
Export logs	Select to export logs to your local hard disk drive (HDD) in `.log` format.
Clear logs	Select to clear all logs. You will be presented a confirmation window, select *Yes* to proceed.

Configure Antivirus options

In standalone mode, you can configure additional settings for the *Antivirus* tab by using the *File* > *Settings* page. See Antivirus options on page 104.

In managed mode, Antivirus options are controlled by the profile assigned to the endpoint by FortiGate or EMS.

Web Security/Web Filter

Web Security/Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FortiGuard Distribution Network (FDN). You can create a custom URL filter exclusion list which overrides the FDN category.

When a FortiClient endpoint is connected to FortiGate or EMS, the *Web Security* tab becomes the *Web Filter* tab in the FortiClient console.

Enable/disable Web Security/Web Filter

For FortiClient in standalone mode, you can enable, disable, and configure web security by using the FortiClient console. You can define what sites are allowed, blocked, or monitored, and you can view violations.

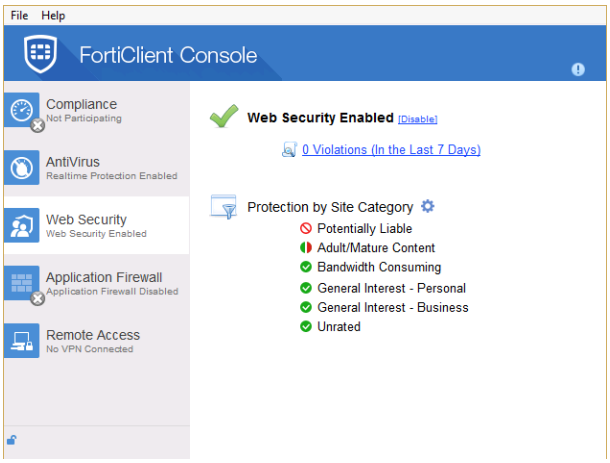
For FortiClient in managed mode, an administrator enables, disables, and configures Web Filter by using a FortiClient profile. See FortiClient profiles on page 26.

Enable/disable Web Security

This setting can only be configured when FortiClient is in standalone mode.

To enable or disable Web Security:

1. On the *Web Security* tab, toggle the *Enable/Disable* link in the FortiClient console. Web Security is enabled by default.



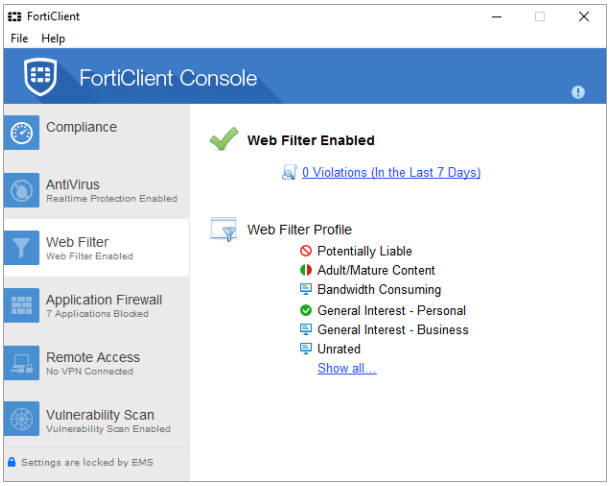
The following options are available:

Enable/Disable	Select to enable or disable Web Security.

X Violations (In the Last 7 Days)	Select to view Web Security log entries of the violations that have occurred in the last 7 days.
Settings	Select to configure the Web Security profile, exclusion list, and settings, and to view violations.

Enable/disable Web Filter

This setting can only be configured when FortiClient is in managed mode. When FortiClient is connected to a FortiGate or EMS, the *Web Security* tab will become the *Web Filter* tab.



You can disable *Web Filter* in FortiClient from the FortiGate FortiClient profile. You can also select to enable or disable Web Filter when the FortiClient device is On-Net. When *FortiGuard Categories* is disabled, FortiClient will be protected by the *Exclusion List* configured in the URL in the FortiClient profile.

A FortiClient profile can include a Web Filter profile from a FortiGate or EMS.

On a FortiGate device, the overall process is as follows:

- Create a Web Filter profile on the FortiGate,
- Add the Web Filter profile to the FortiClient Profile on the FortiGate.

On EMS, web filtering is part of the endpoint profile.

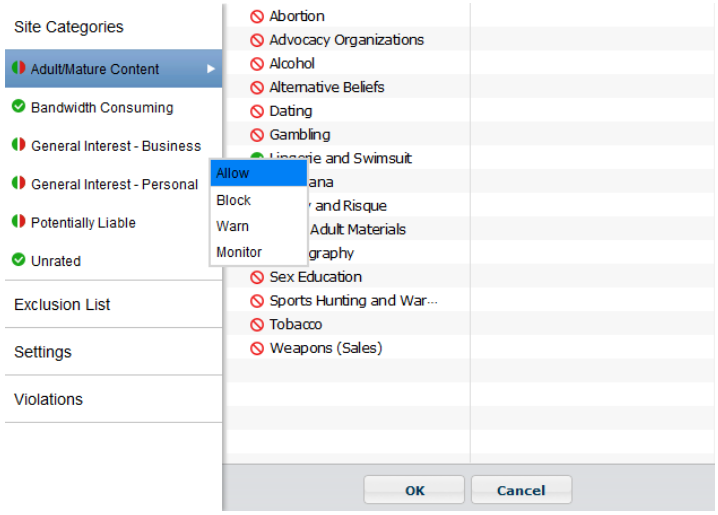
Configure Web Security profiles

This setting can only be configured when FortiClient is in standalone mode.

You can configure a Web Security profile to allow, block, warn, or monitor web traffic based on website categories and sub-categories.

To configure web security profiles:

1. On the *Web Filter* tab, click the *Settings* icon.
2. Click a site category.
3. Click the *Action* icon, and select an action in the drop-down menu.



The following actions are available:

Allow	Set the category or sub-category to *Allow* to allow access.
Block	Set the category or sub-category to *Block* to block access. The user will receive a Web Page Blocked message in the web browser.
Warn	Set the category or sub-category to *Warn* to block access. The user will receive a Web Page Blocked message in the web browser. The user can select to proceed or go back to the previous web page.
Monitor	Set the category or sub-category to *Monitor* to allow access. The site will be logged.

You can select to enable or disable *Site Categories* in the *Web Security* settings page. When site categories are disabled, FortiClient is protected by the exclusion list.

4. Click *OK*.

Edit Web Security exclusion lists

This setting can only be configured when FortiClient is in standalone mode.

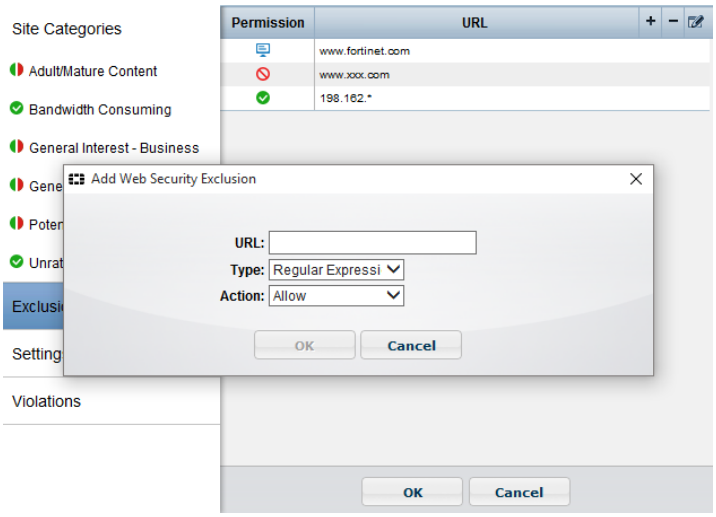
You can add websites to the exclusion list and set the permission to allow, block, monitor, or exempt.

For more information on URL formats, type, and action, see the *FortiOS Handbook* in the Fortinet Document Library.

To manage the exclusion list:

1. On the *Web Security* tab, click the *Settings* icon.
2. Click the *Exclusion List* tab.
3. Click the *Add* icon to add URLs to the exclusion list.

   If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.



4. Configure the following settings:

Exclusion List	Select to exclude URLs that are explicitly blocked or allowed. Use the add icon to add URLs and the delete icon to delete URLs from the list. Select a URL and select the edit icon to edit the selection.
URL	Enter a URL or IP address.
Type	Select one of the following pattern types from the drop-down list: • *Simple* • *Wildcard* • *Regular Expression*
Actions	Select one of the following actions from the drop-down list: • *Block*: Block access to the web site regardless of the URL category or sub-category action. • *Allow*: Allow access to the web site regardless of the URL category or sub-category action. • *Monitor*: Allow access to the web site regardless of the URL category or sub-category action. A log message will be generated each time a matching traffic session is established.

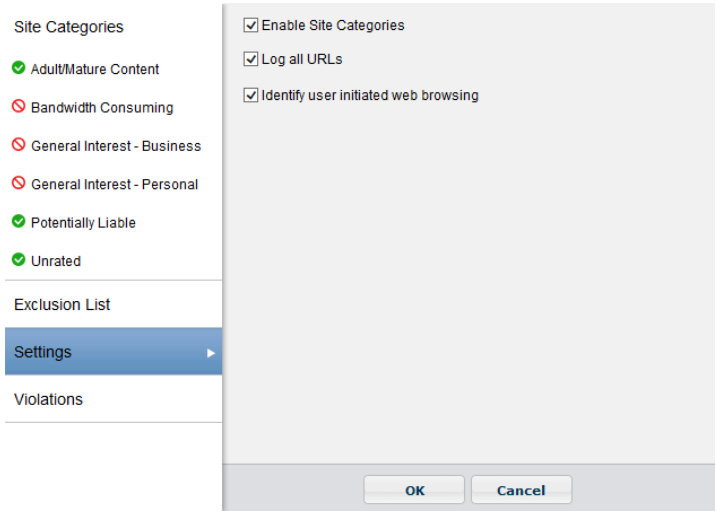
5. Click *OK*.

Configure Web Security settings

This setting can only be configured when FortiClient is in standalone mode.

To configure web security settings:

1. On the *Web Security* tab, click the *Settings* icon
2. Click the *Settings* tab.



3. Configure the following settings:

Enable Site Categories	Select to enable Site Categories. When site categories are disabled, FortiClient is protected by the exclusion list.
Log all URLs	Select to log all URLs.
Identify user initiated web browsing	Select to identify web browser that is user initiated.

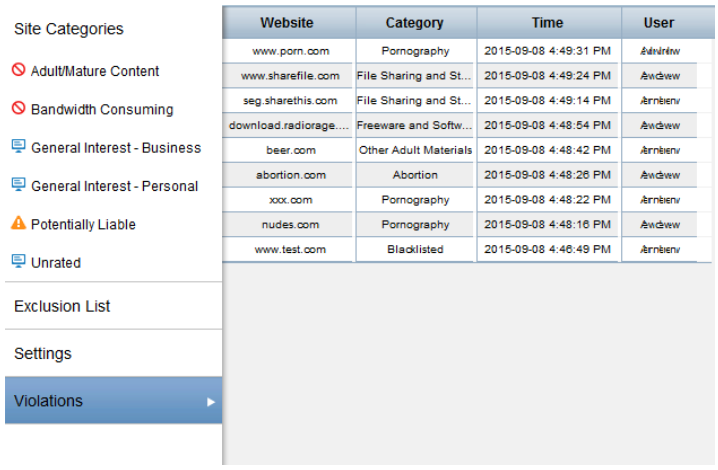
4. Click *OK*.

View violations

This section applies to FortiClient in standalone mode and managed mode.

To view Web Security violations:

1. On the *Web Security* tab, click the *Settings* icon.
   Alternately, you can click the *X Violations (In the Last 7 Days)* link.
2. Click the *Violations* tab.



The following information is displayed.

Website	The website name or IP address.
Category	The website sub-category.
Time	The date and time that the website was accessed.
User	The name of the user generating the traffic. Hover the mouse cursor over the column to view the complete entry in the pop-up bubble message.

3. Click *Close*.

Application Firewall

The section applies only to FortiClient in managed mode.

FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application.

Enable/disable Application Firewall

The administrator enables the application firewall feature by using a FortiClient profile. The FortiClient profile includes the application firewall configuration.

The FortiClient Endpoint Control feature enables the site administrator to distribute an Application Control sensor from FortiGate or EMS.

On the FortiGate, the process is as follows:

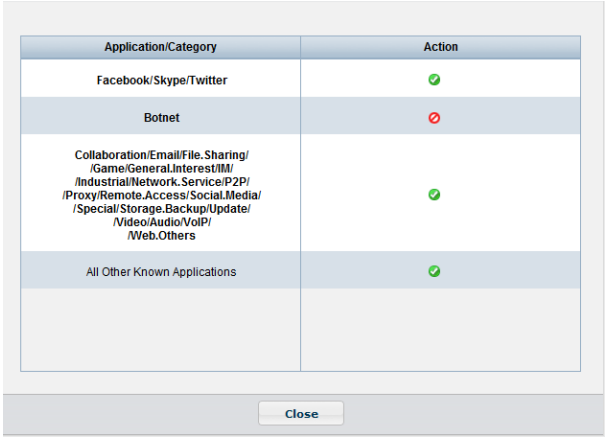
- Create an Application Sensor and Application Filter on the FortiGate,
- Add the Application Sensor to the FortiClient Profile on the FortiGate.

On EMS, the application firewall is part of the endpoint profile.

For more information on configuring application control security profiles, see the *FortiOS Handbook - The Complete Guide to FortiOS* available in the Fortinet Document Library.

View application firewall profiles

To view the application firewall profile, select *Show all*.



View blocked applications

To view blocked applications, select the *Applications Blocked* link in the FortiClient console. This page lists all applications blocked in the past seven days, including the count and time of last occurrence.

IPsec VPN and SSL VPN

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. Administrators can provision client VPN connections to FortiGate in profiles from EMS, and you can configure new connections in FortiClient console.

Add new connections

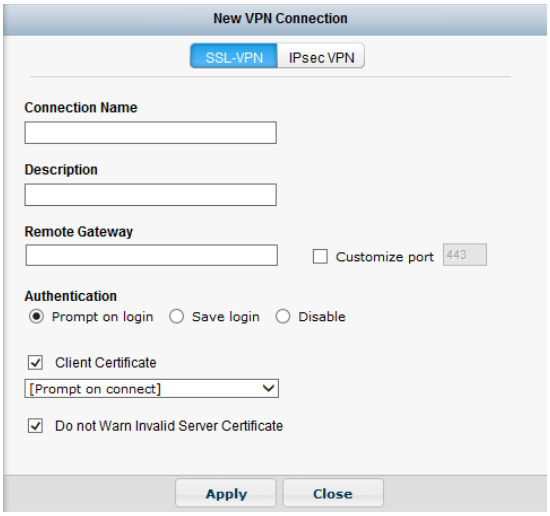
You can add new SSL VPN connections and IPsec VPN connections.

In managed mode, the profile might include VPN configurations from EMS on the *VPN* tab for you to use.

Create SSL VPN connections

To create SSL VPN connections:

1. On the *Remote Access* tab, click the *Configure VPN* link, or use the drop-down menu in the FortiClient console.



2. Select *SSL-VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	Enter a description for the connection. (optional)

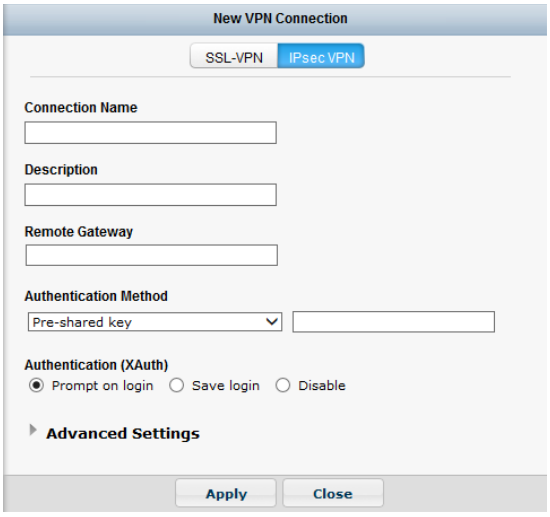
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Customize port	Select to change the port. The default port is 443.
Authentication	Select to prompt on login, or save login. The option to disable is available when *Client Certificate* is enabled.
Username	If you selected to save login, enter the username in the dialog box.
Client Certificate	Select to enable client certificates, then select the certificate from the drop-down list.
Do not Warn Invalid Server Certificate	Select if you do not want to warned if the server presents an invalid certificate.
Add	Select the add icon to add a new connection.
Delete	Select a connection and then select the delete icon to delete a connection.

3. Click *Apply* to save the VPN connection, and then click *Close* to return to the Remote Access screen.

Create IPsec VPN connections

To create IPsec VPN connections:

1. On the *Remote Access* tab, click the *Configure VPN* link, or use the drop-down menu in the FortiClient console.



2. Select *IPsec VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	Enter a description for the connection. (optional)

Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Authentication Method	Select either *X.509 Certificate* or *Pre-shared Key* in the drop-down menu.
Authentication (XAuth)	Select to prompt on login, save login, or disable.
Username	If you selected save login, enter the username in the dialog box.
Advanced Settings	Configure VPN settings, Phase 1, and Phase 2 settings.
VPN Settings	
Mode	Select one of the following: • *Main*: In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*: In Aggressive mode, the phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although *Main* mode is more secure, you must select *Aggressive* mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID).
Options	Select one of the following: • *Mode Config*: IKE Mode Config can configure host IP address, Domain, DNS and WINS addresses. • *Manually Set*: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP, assign IP address, and subnet values. Select the check box to enable split tunneling. • *DHCP over IPsec*: DHCP over IPsec can assign an IP address, Domain, DNS and WINS addresses. Select the check box to enable split tunneling.
Phase 1	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists.

	DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the Local ID (optional). This Local ID value must match the peer ID value given for the remote VPN peer's Peer Options.
	Dead Peer Detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the check box if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Phase 2		Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists.
	Key Life	The Key Life setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
	Enable Perfect Forward Secrecy (PFS)	Select the check box to enable Perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5 or 14). This must match the DH Group that the remote peer or dialup client uses.
Add		Select the add icon to add a new connection.
Delete		Select a connection and then select the delete icon to delete a connection.

3. Click *Apply* to save the VPN connection, and then click *Close* to return to the Remote Access screen.

Connect to VPNs

Microsoft Internet Explorer's SSL and TLS settings should be the same as those on the FortiGate.

To connect to VPNs:

1. On the *Remote Access* tab, select the VPN connection from the drop-down menu.
2. Enter your username, password, and click *Connect*.

Provisioned VPN connections will be listed under *Corporate VPN*. Locally configured VPN connections will be listed under *Personal VPN*.

Optionally, you can click the system tray, and then right-click the FortiClient icon, and select the VPN connection.

You can also select to edit an existing VPN connection and delete an existing VPN connection using the drop-down menu.

When connected, the console will display the connection status, duration, and other relevant information. You can now browse your remote network. Select the *Disconnect* button when you are ready to terminate the VPN session.

Access to certificates in Windows Certificates Stores

On a Windows system, you can view certificates by using an MMC (Microsoft Management Console) snap-in called Certificates console. For more information, see the following Microsoft TechNet articles:

- *Add the Certificates Snap-in to an MMC* available at https://technet.microsoft.com/en-us/library/cc754431
- *Display Certificate Stores* available at https://technet.microsoft.com/en-us/library/cc725751

The Certificates console offers the following snap-in options:

- My user account
- Service account
- Computer account

You can select one or more snap-in options, and they will display in the Certificates console. FortiClient typically searches for certificates in one of the following accounts:

- User account – contains certificates for the logged on user
- Computer account – contains certificates for the local computer

If the certificate is in the local computer account, FortiClient can typically access the certificate. A certificate from the local computer account may be used to establish an IPsec VPN connection, regardless of whether the logged on user is an administrator or a non-administrator. For SSL VPN, the administrator needs to grant permission to users who are non-administrators to access the private key of the certificate. Otherwise, non-administrators

cannot use the certificate in the computer account to establish SSL VPN connections. This restriction does not apply to any user with administrator level permission. IPsec VPN does not have this exception.

If the certificate is in the user account, FortiClient can access the certificate, if the user has already successfully logged in, and the same user imported the certificate. In all other scenarios, FortiClient might be unable to access the certificate.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate for users who are logged into the endpoint and connecting VPN tunnels:

Account	Connect VPN by Using FortiClient GUI or FortiTray	
	Logged in user: Administrator	Logged in user: Non-Administrator
User account	Yes certificate found, if the certificate was imported by the same administrator user	Yes certificate found, if the certificate was imported by the same user
Computer account	Yes certificate found	IPsec VPN: Yes certificate found SSL VPN: Yes certificate found, if access permission granted to private key
SmartCard	Yes certificate found, if same user that was logged on at the time card was inserted	Yes certificate found, if same user that was logged on at the time card was inserted

When a user imports a certificate into the user account, a different logged on user cannot access the same certificate.

A certificate on a smart card is imported into the user account of the logged on user. As a result, the same conditions apply as with the user account.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate before a user logs into the endpoint:

Account	Unknown User Before Logging Into Windows
User account	No certificate found
Computer account	Yes certificate found
SmartCard	No certificate found

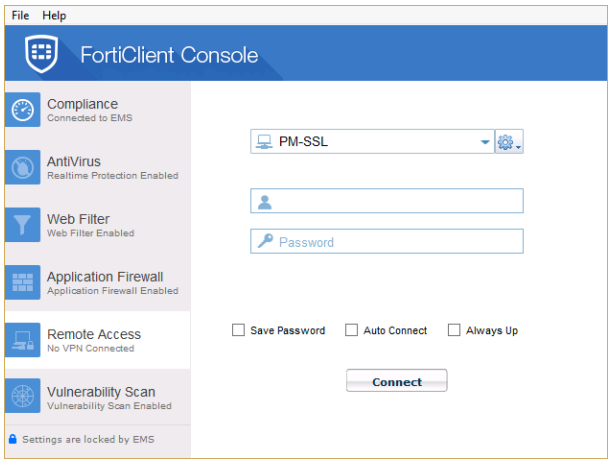
Save password, auto connect, and always up

When configuring a FortiClient IPsec or SSL VPN connection on your FortiGate/EMS, you can select to enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection will automatically connect.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate will sense when the VPN connection is available and re-connect.

For SSL VPN tunnel mode configurations these features are enabled/disabled in the *SSL VPN Portal*.

When enabled in the FortiGate configuration, once the FortiClient is connected to the FortiGate, the client will receive these configuration options.



For FortiClient VPN configurations, once these features are enabled they may only be edited from the command line. Use the following FortiOS CLI commands to disable these features:

```
config vpn ipsec phase1-interface
   edit [vpn name]
      set save-password disable
      set client-auto-negotiate disable
      set client-keep-alive disable
   end
end
```

Advanced features (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference*.

Activate VPN before Windows Log on

When using VPN before Windows log on, the user is offered a list of pre-configured VPN connections to select from on the Windows log on screen. This requires that the Windows log on screen is not bypassed. As such, if VPN before Windows log on is enabled, it is required to also check the check box *Users must enter a user name and password to use this computer* in the *User Accounts* dialog box.

To make this change, proceed as follows:

In FortiClient:

1. Create the VPN tunnels of interest or connect to FortiClient EMS, which provides the VPN list of interest
2. Enable VPN before log on to the FortiClient Settings page, see VPN options on page 104.

On the Microsoft Windows system,

1. Start an elevated command line prompt.
2. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
3. Check the check box for *Users must enter a user name and password to use this computer*.
4. Click *OK* to save the setting.

Connect VPNs before logging on (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then log on to AD/Domain.

```
<forticlient_configuration>
   <vpn>
      <options>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
      </options>
   </vpn>
</forticlient_configuration>
```

Create redundant IPsec VPNs

To use VPN resiliency/redundancy, you will configure a list of VPN gateways, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
            <options>
            ...
            </options>
               <connections>
                  <connection>
                     <name>psk_90_1</name>
                     <type>manual</type>
                     <ike_settings>
                     <prompt_certificate>0</prompt_certificate>
                     <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                     <redundantsortmethod>1</redundantsortmethod>
                     ...
               </ike_settings>
            </connection>
```

```
            </connections>
         </ipsecvpn>
      </vpn>
   </forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Create priority-based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
   <forticlient_configuration>
      <vpn>
         <sslvpn>
            <options>
               <enabled>1</enabled>
               ...
            </options>
            <connections>
               <connection>
                  <name>ssl_90_1</name>
                  <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
                  ...
               </connection>
            </connections>
         </sslvpn>
      </vpn>
   </forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGate must use the same TCP port.

Advanced features (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference*.

Create redundant IPsec VPNs

To use VPN resiliency/redundancy, you will configure a list of FortiGate or EMS IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
            <options>
            ...
            </options>
               <connections>
                  <connection>
                     <name>psk_90_1</name>
                     <type>manual</type>
                     <ike_settings>
                     <prompt_certificate>0</prompt_certificate>
                     <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                     <redundantsortmethod>1</redundantsortmethod>
                     ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate or EMS which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate or EMS starting with the first in the list.

Create priority-based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
```

```
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGate or EMS must use the same TCP port.

VPN tunnel & script

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on EMS's XML format FortiClient profile. The profile will be pushed down to FortiClient from EMS. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed.

Windows

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: \\192.168.10.3\ftpshare /user:Ted Mosby md c:\test copy
                x:\PDF\*.* c:\test ]]>
         </script>
      </script>
   </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: /DELETE ]]>
         </script>
      </script>
   </script>
</on_disconnect>
```

OS X

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>mac</os>
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
             /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

Vulnerability Scan

The section applies only to FortiClient in managed mode.

FortiClient includes a *Vulnerability Scan* module to check endpoint workstations for known system vulnerabilities. The vulnerability scan results can include:

- List of vulnerabilities for Microsoft operating systems, third-party software, and Microsoft software detected on the endpoint device
- Links to more information
- Links to Microsoft bulletin reports
- Software patches that can be installed to resolve or close detected vulnerabilities

You can scan on-demand. The scan results display a summary of vulnerabilities found in the system with links to more details, including links to the FortiGuard Center (FortiGuard.com) for more information. Links to remediation patches might also be included.

Whether and how remediation patches are applied to endpoints depends on the settings in the FortiClient profile that is assigned to the endpoint. Patches can be automatically applied to the FortiClient endpoint to enforce network compliance, or you can manually apply patches.

For the list of software for which FortiClient can check vulnerabilities, see Appendix E - Vulnerability Patches on page 146.

Enable vulnerability scan

The administrator enables and configures the vulnerability scan feature in a FortiClient profile by using FortiGate or EMS.

Enable vulnerability scan in FortiClient profiles (EMS)

In EMS 1.0.1 and later, the vulnerability scan feature is visible by default in the FortiClient profile. The EMS administrator may choose to enable this feature in the FortiClient profile. The EMS administrator can also schedule vulnerability scans and configure remediation patches to be automatically installed on endpoints. For more information, see the *FortiClient EMS Administration Guide*.

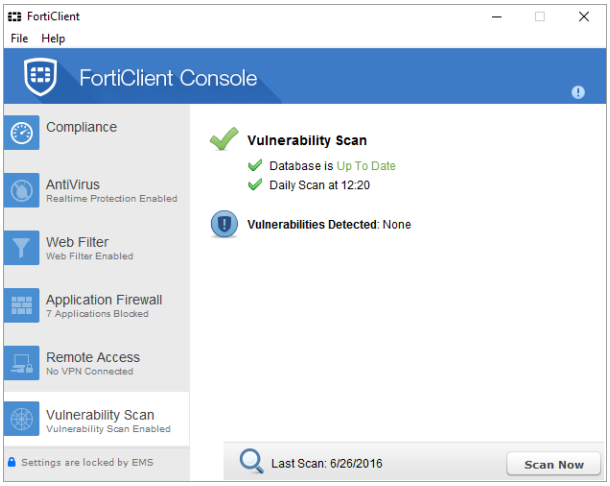
Enable vulnerability scan in FortiClient profiles (FortiGate)

In FortiGate 5.4.1 and later, the vulnerability scan feature is visible by default in the FortiClient profile. The FortiGate administrator may choose to enable this feature in the FortiClient profile.

Scan now

To scan now:

1. In the FortiClient console, click the *Vulnerability Scan* tab.
2. Click the *Scan Now* button. FortiClient scans your workstation for known vulnerabilities.



When the scan is complete, FortiClient displays a summary of vulnerabilities found on the system.

View scan results

Vulnerability scan results are organized into the following categories:

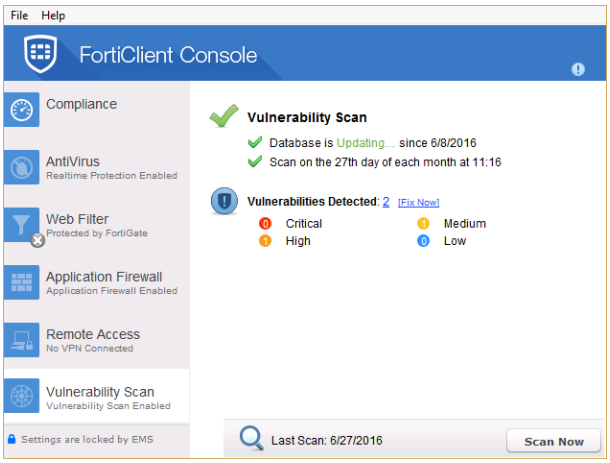
- Critical vulnerabilities
- Vulnerabilities detected

You can use the vulnerability scan results to learn more about vulnerabilities on your computer and to learn what actions you can take to address the vulnerabilities.

When remediation patches are available for software that is running on the managed endpoint, the vulnerability scan results might include the option to install software patches that address the identified vulnerability. See Install remediation patches on page 99.

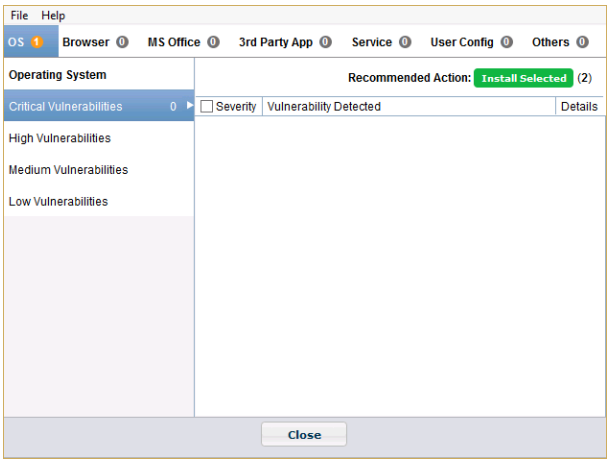
To view scan results:

1. In the FortiClient console, click the *Vulnerability Scan* tab.

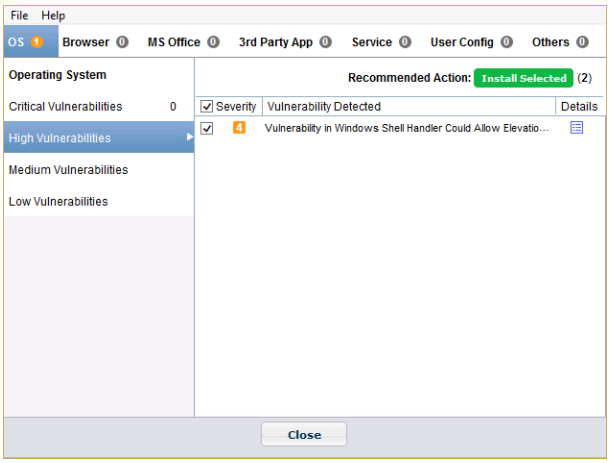


2. Beside *Vulnerabilities Detected*, click the *<number>* link.

   A summary of vulnerabilities detected on your system is displayed.

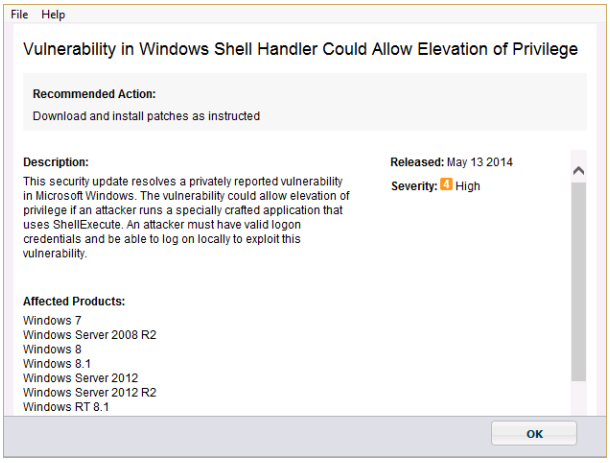


3. Click the tabs, such as *OS*, *Browser*, and so on, to view all vulnerabilities.
4. On each tab, click *Critical Vulnerabilities*, *High Vulnerabilities*, *Medium Vulnerabilities*, and *Low Vulnerabilities* to view the vulnerabilities in each category for each tab.



5. When available, click the *Details* icon to view details about the vulnerability.

   You can scroll to the bottom of the window to click links to more information about CVE IDs and vendor information.



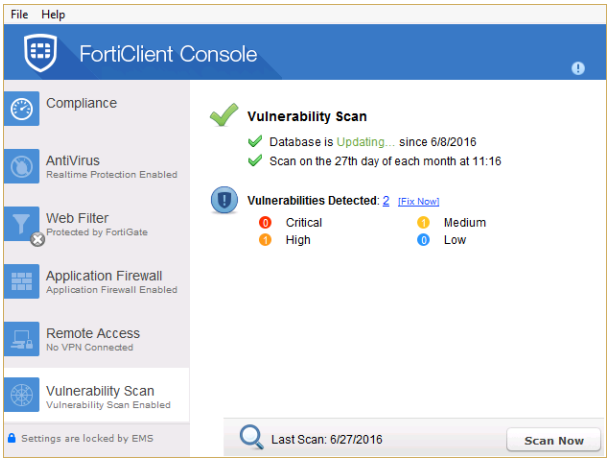
6. Click *OK* to return to the previous screen, and click *Close* to return to the *Vulnerability Scan* tab.

   For information on installing patches, see Install remediation patches on page 99.

View details of scan results

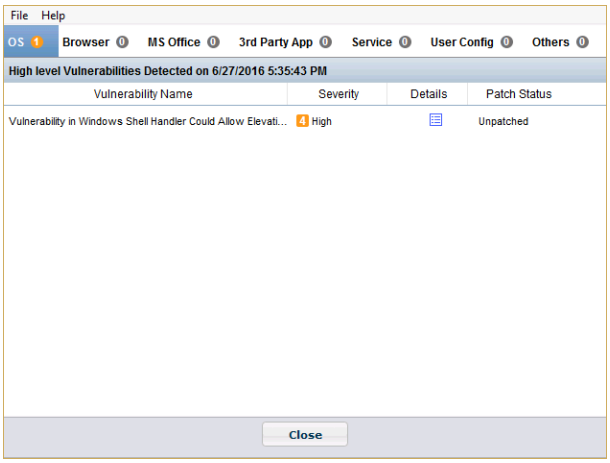
To view details of scan results:

1. In the FortiClient console, click the *Vulnerability Scan* tab.



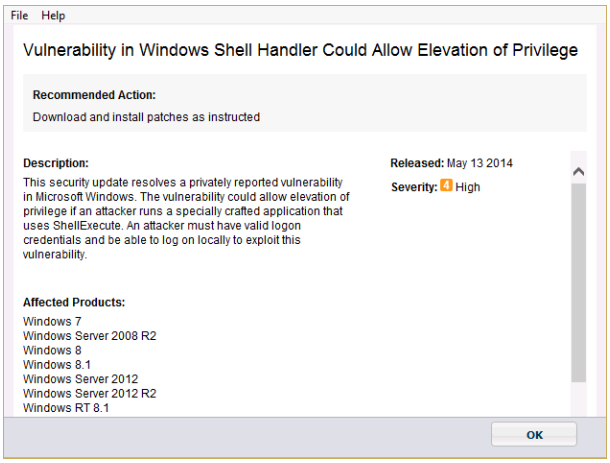
2. Under *Vulnerabilities Detected*, click *Critical*, *High*, *Medium*, or *Low* when the results are greater than 0.

   A summary of vulnerabilities detected on your system is displayed. Click the tabs, such as *OS*, *Browser*, and so on, to view all vulnerabilities.



3. Click the *Details* icon for more information.

   You can scroll to the bottom of the window to click links to more information about CVE (common vulnerabilities and exposures) IDs and vendor information.



4. Click *OK* to return to the previous screen, and click *Close* to return to the *Vulnerability Scan* tab.

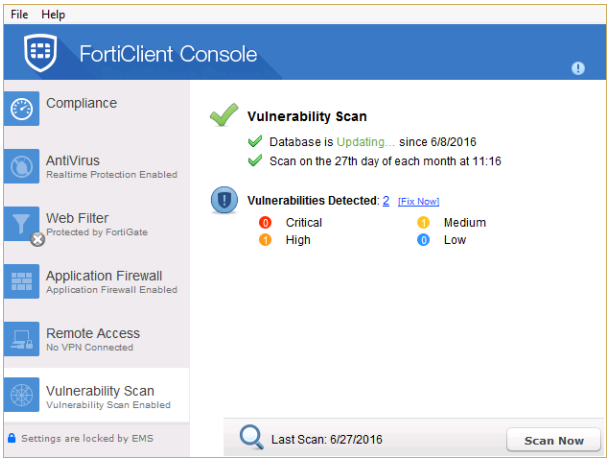
Install remediation patches

When remediation patches are available for software that is running on the managed endpoint, the vulnerability scan results might include the option to install software patches that address the identified vulnerability.

Access to software patches is controlled by the FortiClient profile configuration. Depending on the FortiClient profile settings, the patches might be installed for you, or you might be able to choose what patches to install. In some cases, you must install the software patches to maintain network access. For example, if compliance is configured to block network access for non-compliant endpoints, software patches must be installed to maintain network access.

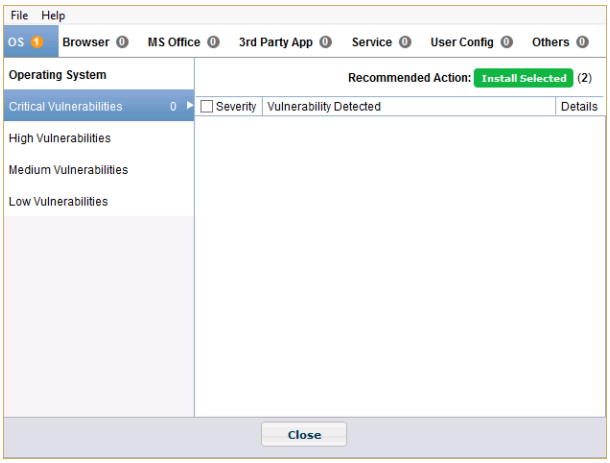
To install remediation patches:

1. In the FortiClient console, click the *Vulnerability Scan* tab.



2. Beside *Vulnerabilities Detected*, click the *<number>* link to review information about vulnerabilities before installing patches.

   Alternately, you can click *Fix Now* to install all remediation patches.



3. Select the check box for each patch that you want to install.

   Click the tabs, such as *OS*, *Browser*, and so on, to view all vulnerabilities. On each tab, click *Critical Vulnerabilities*, *High Vulnerabilities*, *Medium Vulnerabilities*, and *Low Vulnerabilities* to view the vulnerabilities in each category for each tab.

   You may be unable to choose which patches to install, depending on your FortiClient configuration.

4. Click the *Install Selected* button to install the selected patches.

   FortiClient installs the patches. You may need to reboot the endpoint device to complete installation.

Settings

This section describes the available options on the *File* > *Settings* page for FortiClient in standalone mode.

In managed mode, options on the *Settings* page are configured in the FortiClient profile by using FortiGate or EMS.

Backup or restore full configuration

To backup or restore the full configuration file, select *File* > *Settings* from the toolbar. Expand the *System* section, then select *Backup* or *Restore* as needed. *Restore* is only available when operating in standalone mode.

When performing a backup, you can select the file destination, password requirements, and add comments as needed.

Signature updates

This setting can only be configured when FortiClient is in standalone mode.

To configure updates, select *File* > *Settings* from the toolbar, then expand the *System* section.

Select to either automatically download and install updates when they are available on the FortiGuard Distribution Servers, or to send an alert when updates are available.

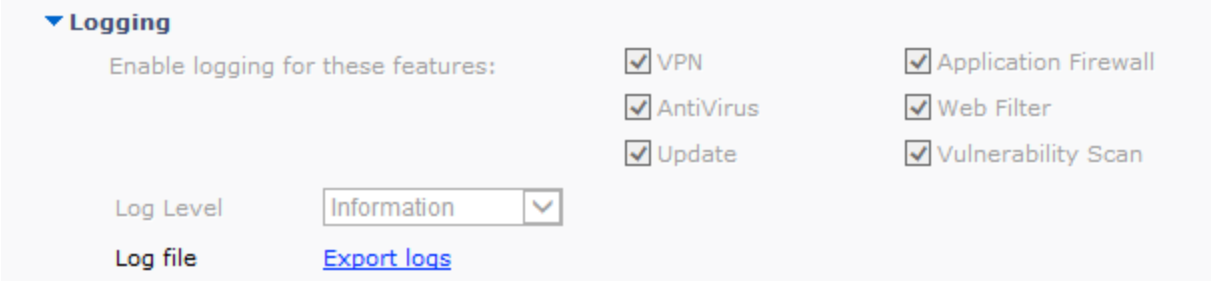
In managed mode, you can select to use a FortiManager device for signature updates. When configuring the endpoint profile in EMS, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

To configure FortiClient to use FortiManager for signature updates (EMS):

1. On EMS, select an endpoint profile, then go to the *System Settings* tab.
2. Toggle the *Use FortiManager for client software/signature update* option to *ON*.
3. Specify the IP address or hostname of the FortiManager device.
4. Select *Failover to FDN when FortiManager is not available* to have FortiClient receive updates from the FortiGuard Distribution Network when the FortiManager is not available.
5. Select *Save* to save the settings.

Logging

To configure logging, select *File* > *Settings* from the toolbar then expand the *Logging* section.



VPN	VPN logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate or EMS.
Application Firewall	Application Firewall logging is available in managed mode when FortiClient is connected to FortiGate or EMS.
AntiVirus	Antivirus activity logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate or EMS.
Web Security/Web Filter	Web Security logging is available when in standalone mode. Web Filter logging is available in managed mode.
Update	Update logging is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate or EMS.
Vulnerability Scan	Vulnerability Scan logging is available in managed mode when FortiClient is connected to FortiGate or EMS.
Log Level	This setting can be configured when in standalone mode. When FortiClient is connected to FortiGate, this setting is set by the XML configuration (if configured).
Log File	The option to export the log file (`.log`) is available when in standalone mode or in managed mode when FortiClient is connected to FortiGate or EMS. The option to clear logs is only available when in standalone mode.

The following table lists the logging levels and description:

Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.

Logging Level	Description
Information	General information about system operations.
Debug	Debug FortiClient.

It is recommended to use the debug logging level only when needed. Do not leave the debug logging level permanently enabled in a production environment to avoid unnecessarily consuming disk space.

Sending logs to FortiAnalyzer or FortiManager

To configure FortiClient to send logs to FortiAnalyzer or FortiManager, you require the following:

- FortiClient 5.2.0 or later
- A FortiGate device running FortiOS 5.2.0 or later or EMS 1.0 or later
- A FortiAnalyzer or FortiManager device running 5.0.7 or later

The connected FortiClient device can send traffic logs, vulnerability scan logs, and event logs to the log device on port 514 TCP.

FortiClient must be connected to FortiGate or EMS to upload logs to FortiAnalyzer or FortiManager.

Some features such as client-based logging when on-net, are only available in the FortiClient profile when a FortiClient 5.2 license has been applied to the FortiGate.

Enable logging on the FortiGate device:

1. On your FortiGate device, select *Log & Report* > *Log Settings*. The *Log Settings* window opens.
2. Enable *Send Logs to FortiAnalyzer/FortiManager*.
3. Enter the IP address of your log device in the *IP Address* field. You can select *Test Connectivity* to ensure your FortiGate is able to communicate with the log device on this IP address.
4. Select *Apply* to save the setting.

FortiClient must be able to access the FortiAnalyzer IP address in order to forward logs.

Enable logging in the FortiGate FortiClient profile:

1. Go to *Security Profiles* > *FortiClient Profiles*.
2. Select the FortiClient Profile and select *Edit* from the toolbar. The *Edit FortiClient Profile* page opens.
3. Enable *Upload Logs to FortiAnalyzer*.
4. Select either *Same as System* to send the logs to the FortiAnalyzer or FortiManager configured in the *Log Settings*, or *Specify* to enter a different IP address.
5. In the *Schedule* field, select to upload logs *Hourly* or *Daily*.

6. Select *Apply* to save the settings.

   Once the FortiClient Profile change is synchronized with the client, you will start receiving logs from connected clients on your FortiAnalyzer/FortiManager system.

   Alternatively, you can configure logging in the command line interface. Go to *System* > *Dashboard* > *Status*. In the *CLI Console* widget, enter the following CLI commands:

```
config endpoint-control profile
   edit <profile-name>
   config forticlient-winmac-settings
      set forticlient-log-upload enable
      set forticlient-log-upload-server <IP address>
      set forticlient-log-upload-schedule {hourly | daily}
      set forticlient-log-ssl-upload {enable | disable}
      set client-log-when-on-net {enable | disable}
   end
end
```

Enable logging in the EMS endpoint profile:

1. On EMS, select an endpoint profile, then go to the *System Settings* tab.
2. Enable *Upload Logs to FortiAnalyzer/FortiManager*.
3. Enable the type of logs to upload. Choose from traffic, vulnerability, and event.
4. Enter the IP address or hostname, schedule upload (in minutes), and log generation timeout (in seconds).
5. Select *Save* to save the settings.

VPN options

To configure VPN options, select *File* > *Settings* from the toolbar and expand the *VPN* section. Select *Enable VPN before logon* to enable VPN before log on.

This setting can only be configured when in standalone mode.

Certificate management

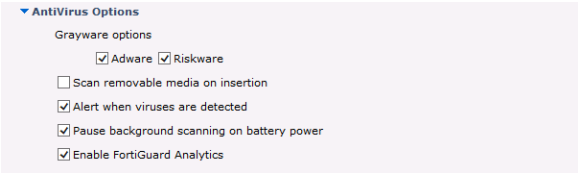
To configure VPN certificates, select *File* > *Settings* from the toolbar and expand the *Certificate Management* section. Select *Use local certificate uploads (IPsec only)* to configure IPsec VPN to use local certificates and import certificates to FortiClient.

This setting can only be configured when in standalone mode.

Antivirus options

To configure antivirus options, select *File* > *Settings* from the toolbar and expand the *Antivirus Options* section.

These settings can be configured only when FortiClient is in standalone mode.



Configure the following settings:

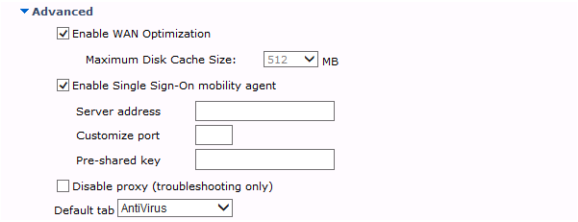
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Scan removable media on insertion	Select to scan removable media when it is inserted.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer. When *Alert when viruses are detected* under *AntiVirus Options* is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.
Pause background scanning on battery power	Select to pause background scanning when your computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

When connected to FortiGate or EMS, you can enable or disable FortiClient Antivirus Protection in the FortiClient profile.

Advanced options

To configure advanced options, select *File* > *Settings* from the toolbar and expand the *Advance* section.

These settings can be configured only when FortiClient is in standalone mode. When a FortiClient endpoint is connected to FortiGate or EMS, these settings are set by the XML configuration (if configured).



Configure the following settings:

Enable WAN Optimization	Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization. This setting can be configured when in standalone mode.
Maximum Disk Cache Size	Select to configure the maximum disk cache size. The default value is 512MB.
Enable Single Sign-On mobility agent	Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device. This setting can be configured when in standalone mode.
Server address	Enter the FortiAuthenticator IP address.
Customize port	Enter the port number. The default port is 8001.
Pre-shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient. This setting can be configured when in standalone mode.
Default tab	Select the default tab to be displayed when opening FortiClient. This setting can be configured when in standalone mode.

Single Sign-On mobility agent

The FortiClient Single Sign-On (SSO) Mobility Agent is a client that updates FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator protocol

The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgment packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- The FortiAuthenticator should be accessible from clients in all locations.
- The FortiAuthenticator should be accessible by all FortiGates.

FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running 2.0.0 or later, or v3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator.

Enable Single Sign-On mobility agent on FortiClient:

1. Select *File* in the toolbar and select *Settings* in the drop-down menu.
2. Select *Advanced* to view the drop-down menu.
3. Select *Enable Single Sign-On mobility agent*.
4. Enter the FortiAuthenticator server address and the pre-shared key.

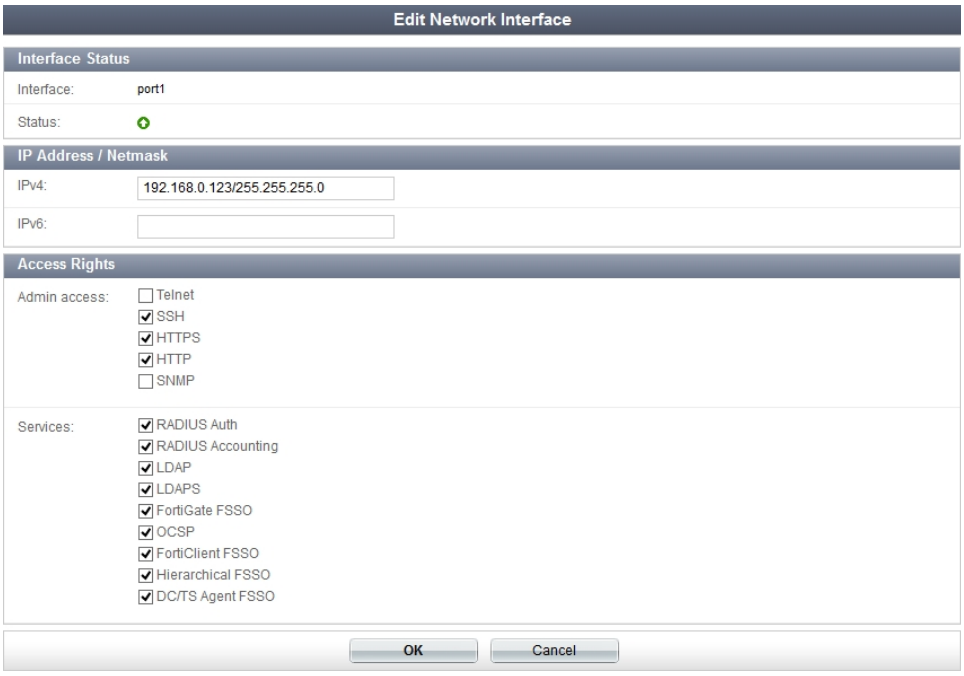
This setting can be configured when in standalone mode. When connected to FortiGate, this setting is set by the XML configuration (if configured).

Enable FortiClient SSO mobility agent service on the FortiAuthenticator:

1. Select *Fortinet SSO Methods* > *SSO* > *General*. The *Edit SSO Configuration* page opens.
2. Select *Enable FortiClient SSO Mobility Agent Service* and enter a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret key or password.
4. Select *OK* to save the setting.

Enable FortiClient FSSO services on the interface:

1. Select *System* > *Network* > *Interfaces*. Select the interface and select *Edit* from the toolbar. The *Edit Network Interface* window opens.



2. Select the checkbox to enable *FortiClient FSSO*.
3. Select *OK* to save the setting.

To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.
For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller.

Configuration lock

To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the *Settings* page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

When the configuration is locked you can perform the following actions:

- Compliance
  - Connect and disconnect FortiClient for Endpoint Control
- Antivirus
  - Complete an antivirus scan, view threats found, and view logs
  - Select *Update Now* to update signatures
- Web Security
  - View violations
- Application Firewall
  - View applications blocked
- Remote Access
  - Configure, edit, or delete an IPsec VPN or SSL VPN connection
  - Connect to a VPN connection
- Vulnerability Scan
  - Complete a vulnerability scan of the system
  - View vulnerabilities found
- Settings
  - Export FortiClient logs
  - Back up the FortiClient configuration

To perform configuration changes, or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration.

FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient console is closed.

- Default menu options:
  - Open FortiClient console

  - Shut down FortiClient
- Dynamic menu options, depending on configuration:
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

When the configuration is locked, the option to shut down FortiClient from FortiTray is grayed out.

Connecting to VPN connections

To connect to a VPN connection from FortiTray, select the Windows System Tray and right-click in the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, then select *OK* to connect.

Diagnostic Tool

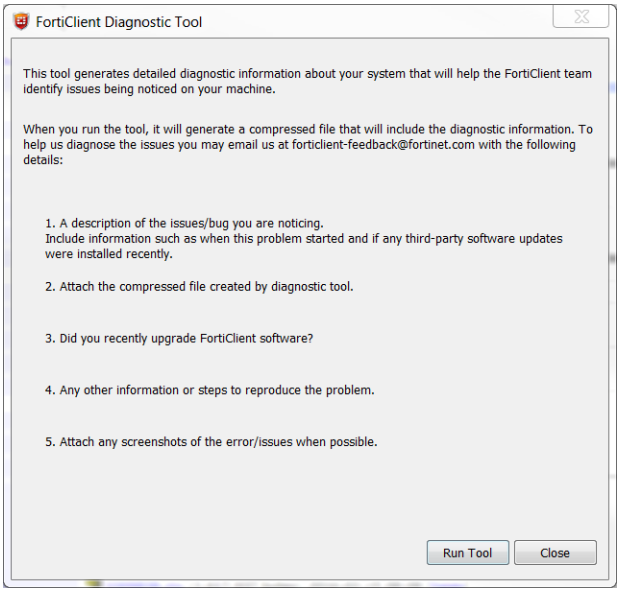
You can access the FortiClient Diagnostic Tool from the FortiClient console. Go to *Help* > *About*.

On FortiClient (Windows), you can also access the Diagnostic Tool from the *Start* menu.

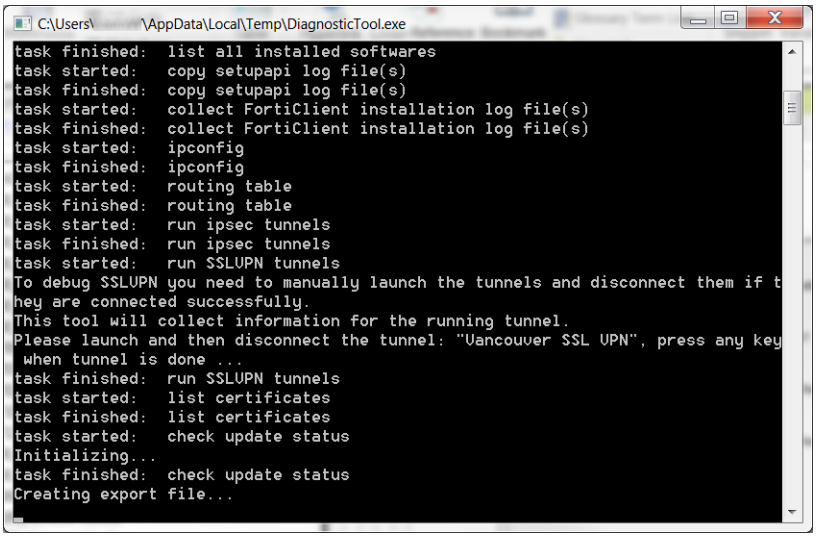
You can use the FortiClient Diagnostic tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and email the report to customer support to help with troubleshooting.

To generate debug reports:

1. Go to *Help* > *About*.
2. Click the *Generate Debug Report* icon in the top-right corner. The FortiClient Diagnostic Tool dialog box is displayed.



3. Click *Run Tool*.
   A window is displayed the provides status information.



4. (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information.

   A *Diagnostic_Result* file is created and displayed in a folder on the endpoint device. The default folder location is *C:\Users <user name>\AppData\Local\Temp*.

5. Click *Close*.

Custom FortiClient Installations

The FortiClient Configurator tool is the recommended method of creating customized FortiClient installation files.

	You can also customize which modules are displayed in the FortiClient dashboard in the FortiClient profile. This will allow you to activate any of the modules at a later date without needing to re-install FortiClient. Any changes made to the FortiClient profile are pushed to connected clients.

	When creating VPN only installation files, you cannot enable other modules in the FortiClient profile as only the VPN module is installed.

	When deploying a custom FortiClient XML configuration, use the advanced profile options in FortiClient EMS to ensure the profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *FortiClient EMS Administration Guide*.

The FortiClient Configurator tool is included with the FortiClient Tools file in FortiClient 5.4.3. This file is only available on the Customer Service & Support portal and is located in the same file directory as the FortiClient images.

The Configurator tool requires activation with a license file. Ensure that you have completed the following steps prior to logging in to your FortiCare product web portal:

- Purchased FortiClient Registration License
- Activated the FortiClient license on a FortiGate

This video explains how to purchase and apply a FortiClient License:
http://www.youtube.com/watch?feature=player_embedded&v=sIkWaUXK0Ok

This chapter contains the following sections:

- Download the license file on page 112
- Prepare configuration files on page 113
- Create a custom installer on page 115
- Custom installation packages on page 122
- Advanced FortiClient profiles on page 123

Download the license file

To retrieve your license file:

1. Go to https://support.fortinet.com and log in to your FortiCare account.
2. Under *Asset* select *Manage/View Products*. Select the FortiGate device that has the FortiClient registration license activated. You will see the *Get the Key File* link in the *Available Key(s)* section.

Registered License(s)

License Type	License Number	Registration Date
FortiClient	FCT102081	2013-08-14
License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series		
SMS	SMS100081	2013-08-16
100 SMS Messages (activation Date:2013-08-16, expiration Date:2014-08-16, number of used:0, number of unused:100)		

Available Key(s)

Key	Description
TK42-NCFS-6NTF-32YF-	License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.0.
TK42-NCFS-6NTF-32YF-	1 Year FortiClient License Subscription for up to 200 clients on FG/FWF 20-90 Series running FortiOS 5.2 and above. Includes the ability to download the license file, edit the FortiClient configuration file and create a custom installer. (expiration Date:2015-04-04)
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.2 and above.

3. Click the link and download license file to your management computer. This file will be needed each time you use the FortiClient Configurator tool.

To use FortiClient Configurator, you need to use a FortiClient 5.4 license file.

Prepare configuration files

You can select the following types of files in the FortiClient Configurator tool:

- Configuration file
- Gateway IP list

This section describes how to retrieve the files and edit them to prepare the files for use with the FortiClient Configurator tool.

Retrieve FortiClient configuration files

You can retrieve a configuration file from FortiClient console. The configuration file contains the settings for FortiClient. After you retrieve the configuration file, you can use an XML editor to make changes to the configuration file. Then you can select the FortiClient configuration file in the FortiClient Configurator tool.

To retrieve FortiClient configuration files:

1. In FortiClient console, go to *File* > *Settings*.
2. In the *System* area, click *Backup*.
3. Select a destination, and click *OK*.
4. Use an XML editor to edit the settings in the configuration file.

For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library, http://docs.fortinet.com.

Configure Telemetry Gateway IP Lists

You can create one or more Telemetry Gateway IP Lists, and then select the list in the FortiClient Configurator tool.

When FortiClient endpoints will connect Telemetry to FortiGate, the Telemetry Gateway IP List contains IP addresses for FortiGate devices.

When FortiClient endpoints will connect Telemetry to FortiGate and send notifications to FortiClient EMS, the Telemetry Gateway IP List contains IP addresses for FortiGate devices and a server notification address for FortiClient EMS.

You use an XML editor to create Telemetry Gateway IP Lists that you can select in the FortiClient Configurator tool.

To configure Telemetry Gateway IP Lists:

1. In FortiClient console, export the configuration. See Retrieve FortiClient configuration files on page 113.
2. Open the configuration file in an XML editor.
3. Remove all elements, except the elements needed to configure the Telemetry Gateway IP List. See Example XML of Telemetry Gateway IP List on page 115.
4. Add IP addresses to the configuration file by using an XML editor.

   When using only FortiGate for endpoint control, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices.

   When using FortiGate integrated with EMS, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices, and use the `<notification_server>` element to identify the IP address for EMS.
5. Save the configuration file.

Example XML of Telemetry Gateway IP List

Following is an example XML file for a Telemetry Gateway IP List. In this example, FortiClient endpoints will connect Telemetry to FortiGate by using the IP addresses in the `<fortigate>` element and send notifications to FortiClient EMS by using the `<notification_server>` element.

```
<?xml version="1.0" encoding="UTF-8" ?>
   <forticlient_configuration>
      <endpoint_control>
         <enabled>1</enabled>
         <disable_unregister>0</disable_unregister>
         <silent_registration>1</silent_registration>
         <fortigates>
            <fortigate>
               <serial_number>fgt_sn0</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                   da7e6495841d8fc9c61067f81ef4cac01d697bb7e160c24d</registration_password>
               <addresses>172.30.254.150:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn1</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                   6c9f088323beef31ea969c1c31c6db0e766273cb21851e68</registration_password>
               <addresses>172.30.254.174:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn2</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                   7e819fa80a68ca2b602fdad54ba76190f03777c70399471d</registration_password>
               <addresses>172.30.254.158:8013</addresses>
            </fortigate>
            <notification_server>
               <address>us-ems1.myfortinet.com:8013</address>
            </notification_server>
         </fortigates>
      </endpoint_control>
   </forticlient_configuration>
```

Create a custom installer

Fortinet offers a repacking tool for both Microsoft Windows and Mac OS X operating systems. The following section provides instructions on creating a custom installer file using the FortiClient Configurator tool.

When selecting to install custom features, only modules selected are installed. To enable other features you will need to uninstall FortiClient, and reinstall an MSI file with these features included in the installer.

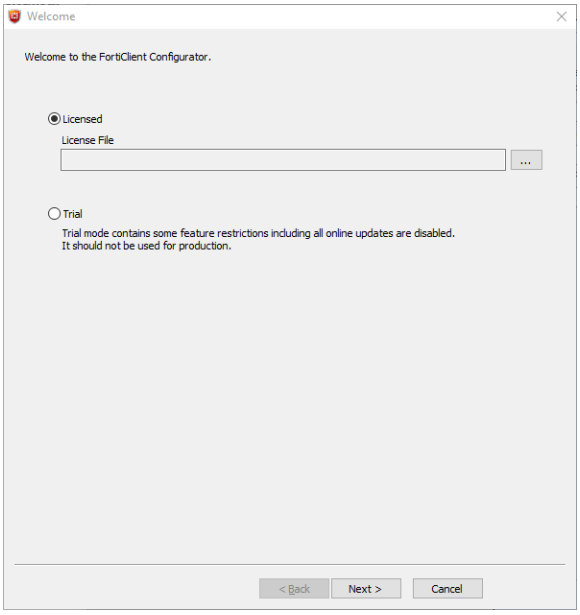
FortiClient (Windows) Configurator tool

Windows has a hard limit of 260 characters on file path length. It is recommended to run the FortiClient Configurator tool in a shallow directory structure, such as c:\temp\, to avoid hitting the hard limit.

To create a custom installer using the FortiClient Configurator tool:

1. Unzip the FortiClientTools file, select the FortiClientConfigurator file folder, and double-click the *FortiClientConfigurator.exe* application file to launch the tool.

   The tool opens at the *Welcome* page.



Licensed	Licensed mode requires a FortiClient license file.
Trial	In FortiClient 5.4, the FortiClient Configurator tool can be used in trial mode. In trial mode, all online updates are disabled. The trial installer is intended to be deployed in a test environment.

2. Browse and select the FortiClient Configurator Activation Key file (`.lic`) on your management computer.

The FortiClient Configurator tool is not installed on the management computer. You must upload the FortiClient Configurator Activation Key file (`.lic`) each time you run the tool.

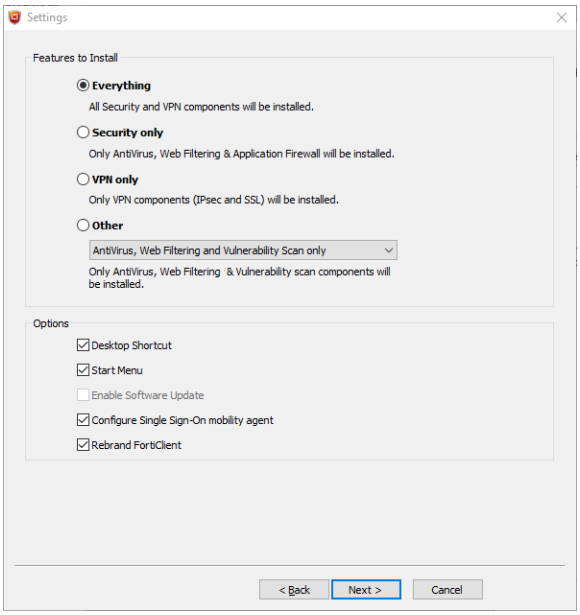
3. After entering the FortiClient Configurator license, select *Next*. The *Configuration File* page is displayed.

Select Config File (optional)	The configuration file (`.conf`, `.sconf`) settings will be included in the installer file.

Password	If the configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
FortiClient Telemetry Gateway IP List (optional)	The FortiClient Telemetry Gateway IP List will be included in the installer file. This option is disabled when using Trial mode.

You can use an XML editor to make changes to the FortiClient configuration file. For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library, http://docs.fortinet.com.

4. Browse and select the FortiClient configuration file on your management computer. This is an optional step. If you do not want to import settings from a configuration file, select *Skip* to continue. The *Settings* page is displayed.



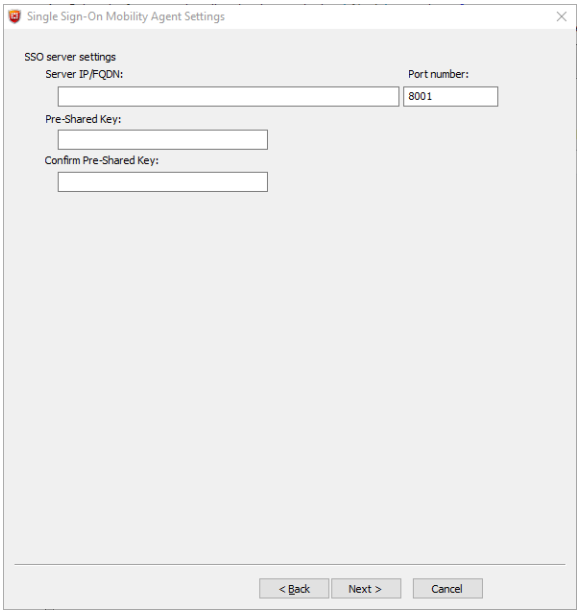
The following options are available for custom installations:

Features to Install	
Everything	All Security and VPN components will be installed.
Security only	Only AntiVirus, Web Filtering, and Application Firewall will be installed.
VPN only	Only VPN components (IPsec and SSL) will be installed.

Features to Install		
	Other	Select one of the following from the drop-down list: • AntiVirus, Web Filtering and Vulnerability Scan only • Web Filtering only • Vulnerability Scan only • Application Firewall only • Application Firewall, Web Filtering and Vulnerability Scan • Application Firewall, VPN, Web Filtering and Vulnerability Scan • Single Sign-On mobility agent only
Options		
	Desktop Shortcut	Select to create a FortiClient desktop icon.
	Start Menu	Select to add FortiClient to the start menu.
	Enable Software Update	Select to enable software updates. This option is disabled when *Rebrand FortiClient* is selected. This option is also disabled when using Trial mode.
	Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator.
	Rebrand FortiClient	Select to rebrand FortiClient. When selected, the option to enable software update is not available. For more information on rebranding FortiClient, see Appendix C - Rebrand FortiClient on page 129.

5. Select the features to install and options and select *Next* to continue.

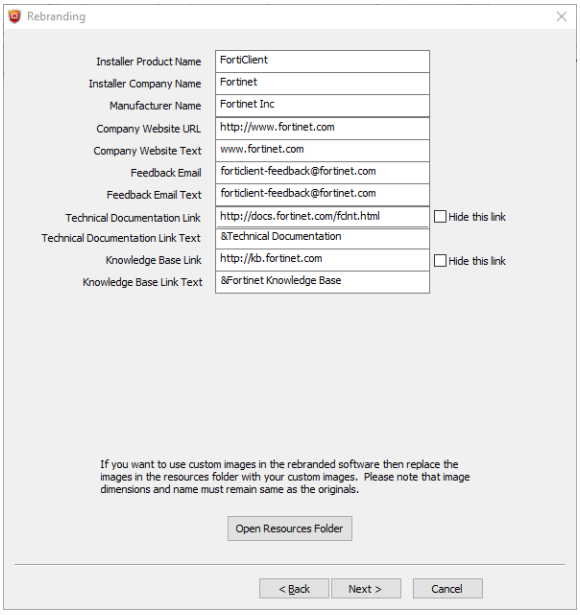
   If you selected to configure the single sign-on mobility agent, the *Single Sign-On Mobility Agent Settings* page is displayed.



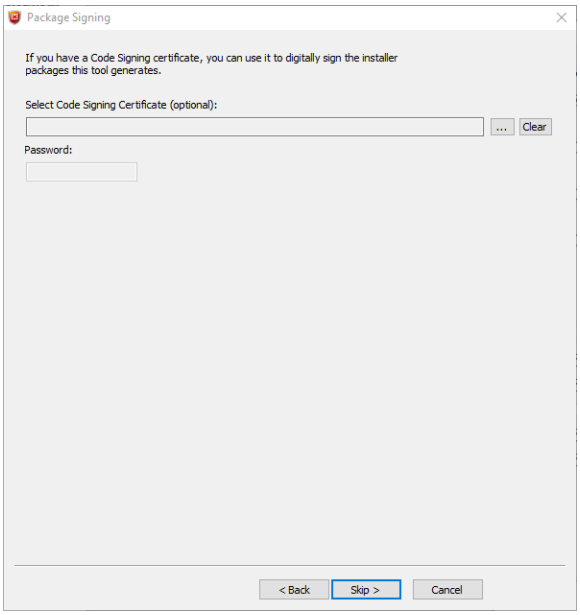
6. Configure the following settings:

Server IP/FQDN	Enter the IP address or FQDN of the FortiAuthenticator server.
Port Number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

7. Select *Next* to continue. If you selected to rebrand FortiClient, the *Rebranding* page is displayed.



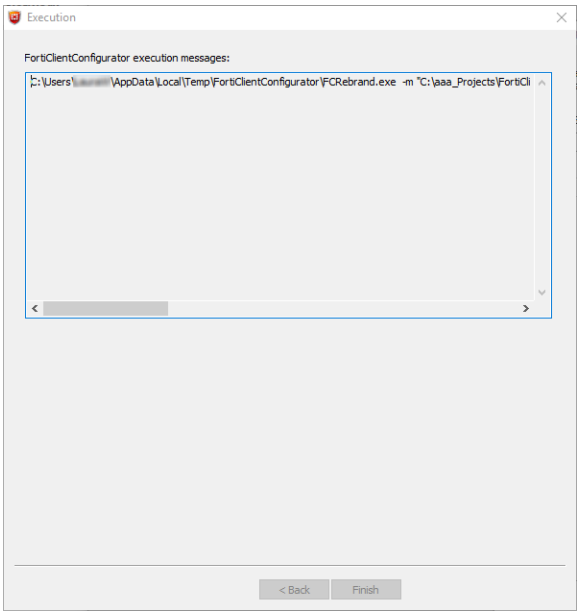
8. Rebrand FortiClient elements as required. The resources folder contains graphical elements. For more information, see Appendix C - Rebrand FortiClient on page 129.
9. Select *Next* to continue. The *Package Signing* page is displayed.



10. Configure the following settings:

Select Code Signing Certificate (optional)	If you have a code signing certificate, you can use it to digitally sign the installer package this tool generates.
Password	If the certificate file is password protected, enter the password.

11. Browse and select the code signing certificate on your management computer. This is an optional step. If you do not want to digitally sign the installer package, select *Skip* to continue. The *Execution* page is displayed.



This page provides details of the installer file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

12. When you select *Finish*, the folder containing the newly created MSI file will open.

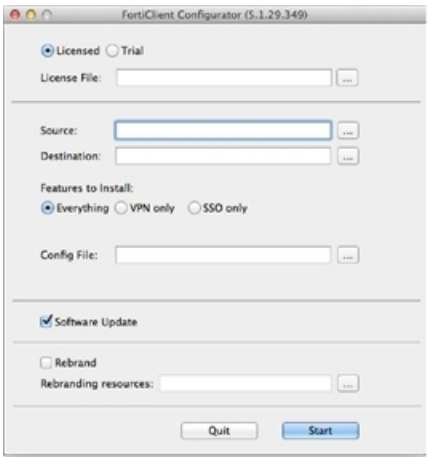
Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly. In FortiClient 5.2.0 and later, an `.exe` installation file is created for manual distribution.

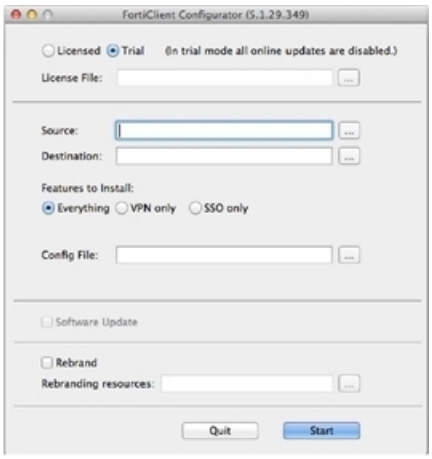
Installation files are organized in folders within the *FortiClientTools* > *FortiClient Configurator* > *FortiClient repackaged* folder. Folder names identify the type of installation files that were created and the creation date.

FortiClient (Mac OS X) Configurator tool

To create a custom installer using the FortiClient Configurator tool:

1. Unzip the FortiClientTools file, select the Configurator file folder, and double-click the *FortiClientConfigurator.dmg* application file, and double-click the FCTConfigurator icon to launch the tool. The *Configurator* tool opens.



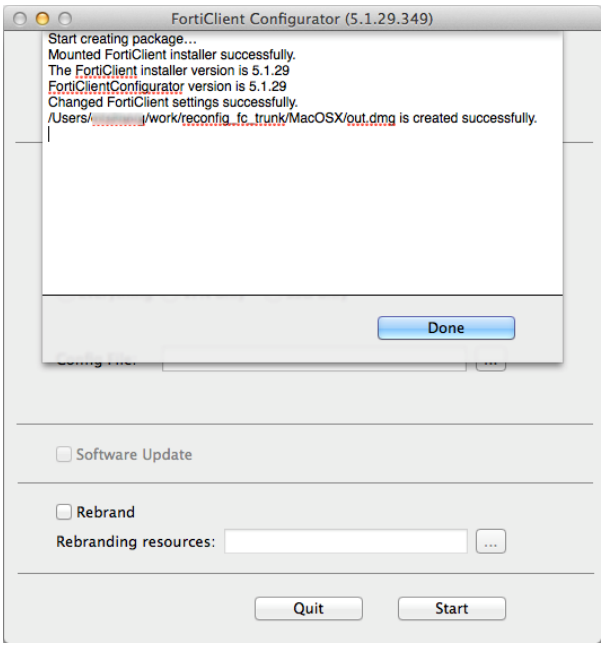


2. Configure the following settings:

Licensed | Trial	Licensed mode requires a FortiClient 5.2 license file. In FortiClient v5.2, the FortiClient Configurator tool can be used in trial mode. In trial mode, all online updates are disabled. The trial installer is intended to be deployed in a test environment.
Source	Select the FortiClient Installer file on your management computer. You must use the full installer file, otherwise FortiClient Configurator will fail to create a custom installation file. The FortiClient Installer version and FortiClient Configurator version must match, otherwise the Configurator will fail to create a custom installation file.
Destination	Enter a name for the custom installation file and select a destination to save the file on your management computer.
Features to Install	Select to install all FortiClient modules, VPN only, or SSO only. If SSO only is selected, you must configure the SSO settings in the attached configuration file.
Server IP/FQDN	Enter the IP address or FQDN of the FortiAuthenticator server. This option is available when selecting SSO only for features to install.
Port Number	Enter the port number. The default port is 8001. This option is available when selecting SSO only for features to install.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key. This option is available when selecting SSO only for features to install.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation. This option is available when selecting SSO only for features to install.
Config file	Optionally, select a pre-configured FortiClient backup configuration file. If you selected *Everything* or *VPN only* for features to install, you must use a configuration file to configure the related settings.
Software Update	Select to enable or disable software updates.

Rebrand	Select to rebrand FortiClient. When selected, the option to enable software update is not available. For more information on rebranding FortiClient, see Appendix C - Rebrand FortiClient on page 129.
Rebranding resources	Select the FortiClient resources file on your management computer.

3. Select the *Start* button to create the custom FortiClient installation file.



4. You can now deploy the repackaged FortiClient `.dmg` file to your Mac OS X systems.

Custom installation packages

When deploying a custom FortiClient XML configuration, you can use the advanced profile options in FortiClient EMS to ensure the profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *FortiClient EMS Administration Guide*.

FortiClient (Windows)

After the FortiClient Configurator tool generates the custom installation packages, you can use the custom installation packages to deploy FortiClient software either manually, or using Active Directory. Both options can be found in the *.../FortiClient_packaged* directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

If you are using Active Directory to deploy FortiClient, you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

For manual distribution, use the `.exe` file in the *.../ManualDistribution* folder.

Advanced FortiClient profiles

When creating custom FortiClient MSI files for deployment, you will need to configure advanced FortiClient profiles on FortiClient EMS to ensure that settings in the FortiClient profile do not overwrite your custom XML settings. You can configure the FortiClient profile to deliver the full XML configuration, VPN only, or specific FortiClient XML configurations. For information on provisioning a full XML configuration file, see Advanced FortiClient profiles on page 1.

For more information on customizing the FortiClient XML configuration file, see the Appendix C - Rebrand FortiClient on page 129.

Fortinet recommends creating OS specific endpoint profiles when provisioning XML settings. When creating a new FortiClient profile, select the device group as either Windows PC or Mac. If a FortiClient (Windows) XML configuration is pushed to a FortiClient (Mac OS X) system, FortiClient (Mac OS X) will ignore settings which are not supported.

Appendix A - Deployment Scenarios

Basic FortiClient profile

In this scenario, you want to configure a FortiClient profile by using the FortiGate GUI. When clients connect FortiClient Telemetry to FortiGate, they will receive the settings configured in the FortiClient profile. You can configure the default profile, or create a new profile. When creating a new profile, you have additional options to specify device groups, user groups, and users.

Create a basic FortiClient profile:

1. In the FortiGate GUI, go to *Security Profiles* > *FortiClient Profiles*. You can either select the default FortiClient profile or select *Create New* in the toolbar.

   The *Edit Endpoint Profile* page opens.

   The default FortiClient profile does not include the *Assign Profile To* setting.

2. Set the profile settings as required, and click *OK*.

Advanced FortiClient profile

In this scenario, you have created a custom XML configuration file. The custom file includes all settings required by the client at the time of deployment. When FortiClient connects Telemetry to FortiGate or EMS, you want to ensure that the client receives the full XML configuration. For future configuration changes, you can edit the XML in the profile by using EMS.

To reduce the size of the FortiClient XML configuration file, you can delete all help text found within the `<!-- .... -->` comment tags.

Create an advanced FortiClient profile with the full XML configuration provisioned:

1. In EMS, go to *Endpoint Profiles* > *Add a new profile*.
2. Select the *Advanced*.
3. (Optional) On *Install* tab, select a FortiClient installer.
4. On the *Configuration* tab, overwrite the XML by pasting the XML from your custom XML configuration file into the pane.
   a. Open the FortiClient XML configuration file in a source code editor.
   b. Copy the FortiClient XML.
   c. Paste the FortiClient XML into the Configuration tab.
5. Click *Save*.

Use Active Directory Groups

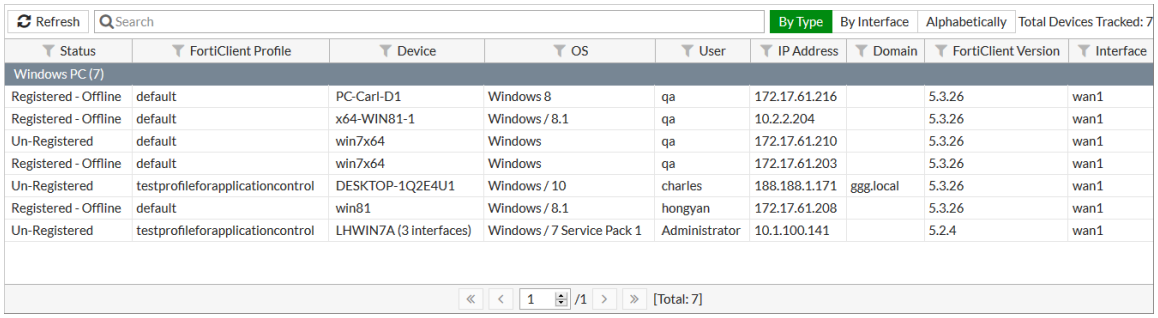
Some organizations may choose to deploy different FortiClient profiles to different user groups. FortiGate and EMS are able to send different FortiClient profiles based on the AD group of the user. This requires use of the FortiAuthenticator.

No special configuration is required on FortiClient.

Monitor connected users

Administrators can monitor managed FortiClient users. When the client successfully connects FortiClient Telemetry to the FortiGate or EMS, the client can be monitored on the FortiGate or EMS.

In the FortiGate GUI, all connected clients can be observed on the *Monitor* > *FortiClient Monitor* page.



Refresh | Search | By Type | By Interface | Alphabetically | Total Devices Tracked: 7

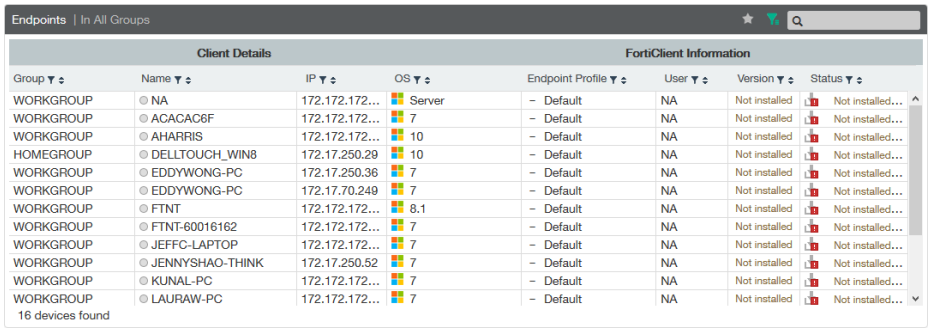
Status	FortiClient Profile	Device	OS	User	IP Address	Domain	FortiClient Version	Interface
Windows PC (7)								
Registered - Offline	default	PC-Carl-D1	Windows 8	qa	172.17.61.216		5.3.26	wan1
Registered - Offline	default	x64-WIN81-1	Windows / 8.1	qa	10.2.2.204		5.3.26	wan1
Un-Registered	default	win7x64	Windows	qa	172.17.61.210		5.3.26	wan1
Registered - Offline	default	win7x64	Windows	qa	172.17.61.203		5.3.26	wan1
Un-Registered	testprofileforapplicationcontrol	DESKTOP-1Q2E4U1	Windows / 10	charles	188.188.1.171	ggg.local	5.3.26	wan1
Registered - Offline	default	win81	Windows / 8.1	hongyan	172.17.61.208		5.3.26	wan1
Un-Registered	testprofileforapplicationcontrol	LHWIN7A (3 interfaces)	Windows / 7 Service Pack 1	Administrator	10.1.100.141		5.2.4	wan1

« ‹ 1 /1 › » [Total: 7]

Either of the following FortiGate CLI commands will list all connected clients:

- `diagnose endpoint registration list`, or
- `diagnose endpoint record-list`.

In the EMS, connected clients can be observed on the *Workgroups* page.



Endpoints | In All Groups

Client Details				FortiClient Information			
Group	Name	IP	OS	Endpoint Profile	User	Version	Status
WORKGROUP	NA	172.172.172...	Server	Default	NA	Not installed	Not installed...
WORKGROUP	ACACAC6F	172.172.172...	7	Default	NA	Not installed	Not installed...
WORKGROUP	AHARRIS	172.172.172...	10	Default	NA	Not installed	Not installed...
HOMEGROUP	DELLTOUCH_WIN8	172.17.250.29	10	Default	NA	Not installed	Not installed...
WORKGROUP	EDDYWONG-PC	172.17.250.36	7	Default	NA	Not installed	Not installed...
WORKGROUP	EDDYWONG-PC	172.17.70.249	7	Default	NA	Not installed	Not installed...
WORKGROUP	FTNT	172.172.172...	8.1	Default	NA	Not installed	Not installed...
WORKGROUP	FTNT-60016162	172.172.172...	7	Default	NA	Not installed	Not installed...
WORKGROUP	JEFFC-LAPTOP	172.172.172...	7	Default	NA	Not installed	Not installed...
WORKGROUP	JENNYSHAO-THINK	172.17.250.52	7	Default	NA	Not installed	Not installed...
WORKGROUP	KUNAL-PC	172.172.172...	7	Default	NA	Not installed	Not installed...
WORKGROUP	LAURAW-PC	172.172.172...	7	Default	NA	Not installed	Not installed...

16 devices found

Customize FortiClient using XML settings

FortiClient configurations can be customized at the XML level. For more information, see the *FortiClient XML Reference*.

Silent connection

You may want to configure FortiClient to silently connect to FortiGate without any user interaction. When configured, the user will not be prompted to connect to a FortiGate. The <silent_registration> tag is intended to be used with the <disable_unregister> tab. For more information, see Disable disconnect on page 126. The following XML elements can be used to enable this:

```
<forticlient_configuration>
   <endpoint_control>
      <silent_registration>1</silent_registration>
   </endpoint_control>
</forticlient_configuration>
```

Disable disconnect

With silent endpoint control connection enabled, a user could disconnect after FortiClient has connected to the FortiGate. The capability to disconnect can be disabled using the following XML element:

```
<forticlient_configuration>
   <endpoint_control>
      <disable_unregister>1</disable_unregister>
   </endpoint_control>
</forticlient_configuration>
```

Put it together

Here is a sample complete FortiClient5.4.3XML configuration file with the capabilities discussed above:

```
<forticlient_configuration>
   <partial_configuration>1</partial_configuration>
   <endpoint_control>
      <enabled>1</enabled>
      <disable_unregister>1</disable_unregister>
      <silent_registration>1</silent_registration>
      <fortigates>
         <fortigate>
            <serial_number />
            <name />
            <registration_password>un9r3Ak@b!e</registration_password>
            <addresses>newyork.example.com</addresses>
         </fortigate>
      </fortigates>
   </endpoint_control>
</forticlient_configuration>
```

The FortiGate that is connected to is listed in the `<fortigates>` element. The `<registration_password>` element is required if the endpoint control configuration on the FortiOS requires one. This can be exported as an encrypted file from a connected FortiClient.

The configuration provided above is not the full FortiClient configuration file. Thus, the `<partial_configuration>` element is set to `1`.

Appendix B - FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API. The API can be used with IPsec VPN only. SSL VPN is currently not supported.

This chapter contains the following sections:

- Overview
- API reference

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - configured tunnel list
  - active tunnel name
  - connected or not
  - idle or not
  - remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN Automation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values.

`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetPolicy pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)`	Command is deprecated in FortiClient v5.0.

`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether keylife time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.
`MakeSystemPolicyCompliant()`	Command is deprecated in FortiClient v5.0.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • User name, Password • True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.

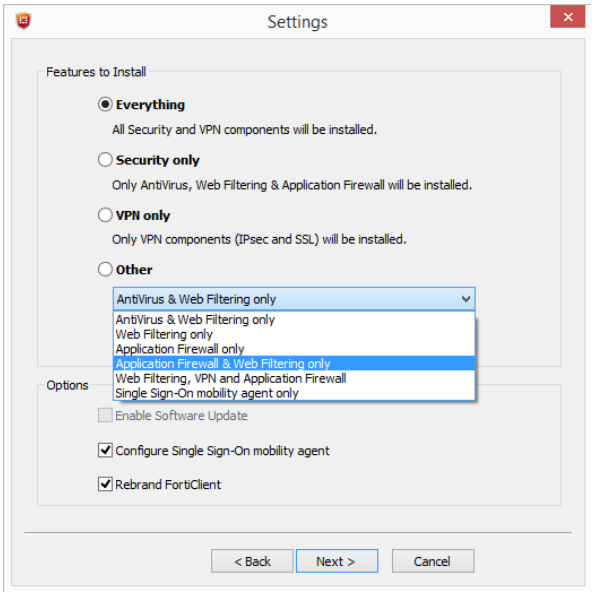
`GetTunnelList()`	Retrieve the list of all connections configured in the FortiClient application.
`IsConnected (bstrTunnelName As String) As Boolean`	Return True if the named connection is up.
`IsIdle (bstrTunnelName As String) As Boolean`	Return True if the named connection is idle.

`OnDisconnect(bstrTunnelName As String)`	Connection disconnected.
`OnIdle(bstrTunnelName As String)`	Connection idle.
`OnOutOfCompliance(bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

Appendix C - Rebrand FortiClient

The FortiClient Configurator can be used to create custom FortiClient MSI installers with various combinations. The customized MSI installer generated may be used to install FortiClient on all supported platforms using Active Directory. A FortiClient setup executable file is also generated for manual distribution.

The FortiClient license for FortiOS 5.2 includes the license file required to use the FortiClient Configurator tool used to create custom FortiClient installers. The Configurator tool also allows you to rebrand the installer file.



Under *Options*, you can select to enable software updates, configure the single sign-on mobility agent, and rebrand FortiClient. Rebranding allows you to edit various UI elements including graphics.

When replacing files in the resource folder, the replacement file should be the same file type and dimensions. Icons (`.ico`) are a special case. The `Main_icon.ico` file for example, is a composite file of multiple icons. The operating system picks the appropriate icon size from this file for the context in which the icon is being displayed.

Rebranding elements:

Installer Product Name	Where Used: Setup Wizard header and body, File directory name in Installer Company Name file folder, engine/signature update bubble messages. Default Value: FortiClient
Installer Company Name	Where Used: File directory name in Program Files. Default Value: Fortinet

Manufacturer Name	Where Used: Default Value: Fortinet Inc
Company WebSite URL	Where Used: *Help* > *About* > *Copyright* page Default Value: http://www.fortinet.com
Company Website Text	Where Used: *Help* > *About* > *Copyright* page Default Value: www.fortinet.com
Feedback Email	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com
Feedback Email Text	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com
Knowledge Base Link	Where used: Link used by Knowledge Base text Default value: http://kb.fortinet.com Leave this field blank to omit the field in the console.
Knowledge Base Link Text	Where Used: Help menu option Default Value: Fortinet Knowledge Base Leave this field blank to omit the field in the console.

Resources folder elements:

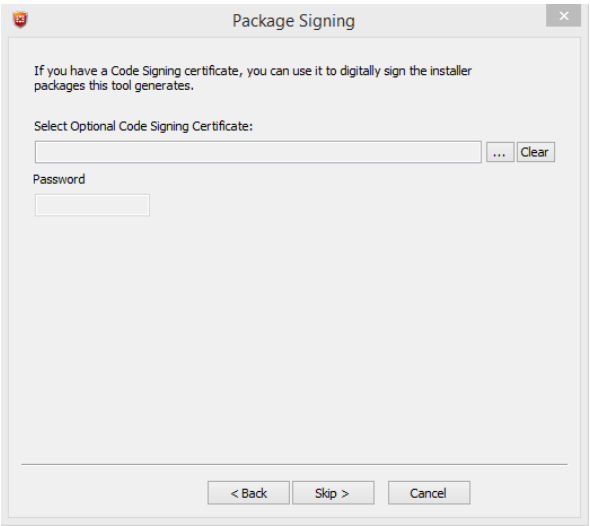
About_red_shield_logo.png	Where Used: File Type: PNG File (.png) Width: 43 pixels Height: 43 pixels Bit Depth: 32
Advertisement_ad_0.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32
Advertisement_ad_1.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels BitBit Depth: 32
Advertisement_ad_2.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32

Antivirus_AV_scan_top_banner_left_hand_side.png	Where Used: File Type: BMP File (.bmp) Width: 1 pixel Height: 40 pixels Bit Depth: 8
Antivirus_AV_scan_top_banner_right_hand_side.png	Where Used: Banner used in right-click “scan with product name” dialog box File Type: BMP File (.bmp) Width: 440 pixels Height: 40 pixels Bit Depth: 8
Common_fgt-not-found-page-bg.png	Where Used: FortiGate not found page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32
Common_fortinet-icon.png	Where Used: File Type: PNG File (.png) Width: 79 pixels Height: 79 pixels Bit Depth: 32
Common_registration_icon.png	Where Used: FortiGate detected page File Type: PNG File (.png) Width: 85 pixels Height: 85 pixels Bit Depth: 32
Common_searching-page-bg.png	Where Used: Searching for FortiGate page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32
Dashboard_forticlient_v5_dashboard_bg.png	Where Used: Client console File Type: PNG File (.png) Width: 628 pixels Height: 451 pixels Bit Depth: 32
Dashboard_warning-shield.png	Where Used: Dashboard warning shield, displayed when antivirus is disabled. File Type: PNG File (.png) Width: 59 pixels Height: 75 pixels Bit Depth: 32

Installer_background.bmp	Where used: Setup Wizard background image. File Type: BMP file (.bmp) Width: 491 pixels Height: 312 pixels Bit Depth: 8
Installer_banner.bmp	Where Used: Setup Wizard banner image on destination page, ready to install page, installing pages. File Type: BMP file (.bmp) Width: 491 pixels Height: 58 pixels Bit Depth: 8
LightInstaller_icon.ico	Where Used: Light Installer Icon File Type: ICO File (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
Main_icon.ico	Where Used: Shortcut on desktop File Type: ICO file (.ico) Width: 48 pixels Height: 48 pixels Bit Depth: 32
Main_logo_black.ico	Where Used: Client console header File Type: ICO file (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
setup.ico	Where Used: Setup icon File Type: ICO File (.ico) Width: 256 pixels Height: 256 pixels Bit Depth: 32
Tray_Icons_alert.ico	Where Used: System tray alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_alert_vpn.ico	Where Used: System tray VPN alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32

Tray_Icons_running.ico	Where Used: System tray running icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_scan1.ico, Tray_Icons_scan2.ico, Tray_Icons_scan3.ico, Tray_Icons_scan4.ico, Tray_Icons_scan5.ico, Tray_Icons_scan6.ico, Tray_Icons_scan7.ico, Tray_Icons_scan8.ico, Tray_Icons_scan9.ico, Tray_Icons_scan10.ico Tray_Icons_scan11.ico	Where Used: System tray, these eleven images animate the scanning activity of the tray icon. File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_vpn.ico	Where Used: System tray VPN icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
VPN_xauth-dialog-logo.png	Where Used: VPN xAuth dialog logo File Type: PNG File (.png) Width: 88 pixels Height: 100 pixels Bit Depth: 32
zzz_rebranding.ini	Where Used: This file is used by the FortiClient Configurator tool for element/resource mapping. File Type: Configuration settings (.ini)

When rebranding FortiClient, you can select to digitally sign the installer package using a code signing certificate.



Appendix D - FortiClient Log Messages

Client Feature	ID	Level	Format	Description
AntiVirus	0x00017913	Warning	Found malware by [AntiVirus scan|AntiVirus realtime protection] in [filesystem|email]	This message is logged when a malware is found.
AntiVirus	0x00017914	Warning	Found suspicious by [AntiVirus scan|AntiVirus realtime protection] in [filesystem|disk|email]	This message is logged when a suspicious is found.
AntiVirus	0x00017915	Info	User enabled Realtime AntiVirus protection	Logged when someone enables Realtime AntiVirus.
AntiVirus	0x00017916	Warning	User disabled Realtime AntiVirus protection	Logged when someone disables Realtime AntiVirus.
AntiVirus	0x00017917	Info	Communication error	
AntiVirus	0x00017918	Warning	AntiVirus realtime protection killed malware process : [process name]	A malware process killed a malware process.
AntiVirus	0x0001791d	Info	av_task scan is started	This message is logged if AV scanning is started.
AntiVirus	0x0001791e	Info	av_task scan is stopped	This message is logged if AV scanning is stopped.
AntiVirus	0x00017919	Info	av_task scan thread is suspended	This message is logged if AV scanning is paused.
AntiVirus	0x0001791a	Info	av_task scan thread is resumed	This message when AV scanning is resumed.
AntiVirus	0x0001791b	Warning	av_task killed suspicious process : <filename or process name>	<filename or process name> is a suspicious process and has been terminated.
AntiVirus	0x0001791c	Info	Cannot start scan task	

Client Feature	ID	Level	Format	Description
AntiVirus	0x0001791f	Error	Scheduled scan failed: Path to file/folder no longer exists.	Path not found.
AntiVirus	0x00017920	Warning	AntiVirus scan was stopped by a user before it finished.	The user specified stopped an AntiVirus scan
AntiVirus	0x00017921	Warning	Failed to connect to FortiSandbox server.	The sandbox server is unavialable
Webfilter	0x000178f4	Info	User enabled Webfilter	Logged when someone enables webfiltering.
Webfilter	0x000178f5	Warning	User disabled Webfilter	Logged when someone disables webfiltering.
Webfilter	0x000178f6	Warning	user's access to the url [action and reason]	the action to the user's access
Webfilter	0x000178f7	Info	user's access to the url [action and reason]	the action to the user's access
Webfilter	0x000178f8	Warning	The Webfilter Violation report was cleared [user name]	Logged when someone clears the webfilter violation report.
Webfilter	0x000178f9	Warning	Unable to create proxy/webfilter communication socket.	FortiClient will not be able to determine the FortiGuard rating of URLs.
Webfilter	0x000178fa	Warning	Unable to retrieve the webfilter UDP port number.	FortiClient will not be able to determine the FortiGuard rating of URLs.
Webfilter	0x000178fb	Warning	status=warn [logged on user] temporarily disabled blocking of category [category id] ([category name]) to access [url]	The user [logged on user] proceeded to the url [url] after acknowledging a warning message.
Application FireWall	0x00017980	Warning	Firewall action	
Application FireWall	0x00017981	Info	Firewall action	
Application FireWall	0x00017982	Info	User enabled Firewall	User enabled Firewall

Client Feature	ID	Level	Format	Description
Application FireWall	0x00017983	Warning	User disabled Firewall	User disabled Firewall
Application FireWall	0x00017984	Warning	The Application Firewall report was cleared	Logged when someone clears the application firewall report.
Application FireWall	0x00017985	Warning	The application firewall has been disabled because it's driver could not be loaded	Logged when application fire-wall driver could not be loaded with error 127 (The specified procedure could not be found).
IKE VPN	0x00017930	Info	VPN tunnel status	VPN tunnel status
IKE VPN	0x00017940	Info	IKE phase1 authentication fail as peer's certificate is not veri-fied.	IKE phase1 authentication fail as peer's certificate is not veri-fied.
IKE VPN	0x00017941	Info	IKE phase1 authentication fail as the preshare key mismatch.	IKE phase1 authentication fail as the preshare key mismatch.
IKE VPN	0x00017931	Warning	No response from the peer	
IKE VPN	0x00017932	Warning	No response from the peer	
IKE VPN	0x00017933	Warning	Received delete payload from peer check xauth password.	Received delete payload from peer check xauth password.
IKE VPN	0x00017934	Error	Failed to acquire an IP address.	Failed to acquire an IP address for the virtual adapter.
IKE VPN	0x00017935	Error	ike error	
IKE VPN	0x00017936	Info	negotiation information	
IKE VPN	0x00017937	Error	negotiation error	
IKE VPN	0x00017938	Error	replayed packet detected (packet dropped)	

Client Feature	ID	Level	Format	Description
IKE VPN	0x00017939	Info	VPN user accept the banner and continue with the tunnel setup	The VPN user accept the banner warning
IKE VPN	0x0001793a	Info	VPN user choose disconnect the tunnel or no response	The VPN user reject the banner warning and disconnect the tunnel
IKE VPN	0x0001793b	Info	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> action=install_sa	
IKE VPN	0x0001793c	Info	VPN before logon was enabled	Logged when someone enables VPN before logon.
IKE VPN	0x0001793d	Info	VPN before logon was disabled	Logged when someone disables VPN before logon.
IKE VPN	0x0001793e	Error	VPN cannot connect because an authorization rule failed.	Logged when a VPN authorization rule failed.
IKE VPN	0x0001793f	Warning	A required application is not running.	VPN cannot connect because the specified application is not running.
SSL VPN	0x00017958	Info	SSLVPN tunnel status	SSLVPN tunnel status
Wan Acceleration	0x00017a71	Info	User enabled WAN Acceleration	User enabled WAN Acceleration
Wan Acceleration	0x00017a70	Info	User disabled WAN Acceleration	User disabled WAN Acceleration
Wan Acceleration	0x0000b000	Error	Network registry keys are missing	When enumerating the network interface subkeys
Wan Acceleration	0x0000b001	Error	Network adapter is missing a description	When enumerating the network interfaces
Wan Acceleration	0x0000b002	Error	Error opening redirector device	Wan acceleration will not function.
Wan Acceleration	0x0000b003	Info	WAN Acceleration was enabled by [user name]	Logged when someone enables WAN Acceleration.

Client Feature	ID	Level	Format	Description
Wan Acceleration	0x0000b004	Info	WAN Acceleration was disabled by [user name]	Logged when someone disables WAN Acceleration.
Vulnerability Scan	0x00017908	Info	The vulnerability scan status has changed	A vulnerability scan status change
Vulnerability Scan	0x00017909	Info	A vulnerability scan result has been logged	A Vulnerability scan result log
Vulnerability Scan	0x0001790a	Info	Remediating vulnerability	The details of the vulnerability being remediated is described by the log fields
EndPoint Control	0x00017ab6	Info	upload logs	
EndPoint Control	0x00017ab7	Info	Endpoint control policy synchronization was enabled	Logged when someone enables Endpoint control policy synchronization.
EndPoint Control	0x00017ab8	Warning	Endpoint control policy synchronization was disabled	Logged when someone disables Endpoint control policy synchronization.
EndPoint Control	0x00017ab9	Info	Endpoint Control Status changed to [status]	Endpoint Control Status Changed
EndPoint Control	0x00017aba	Warning	OffNet configuration version [version] doesn't match FortiGate configuration version [version]	OffNet configuration version doesn't match FortiGate configuration version
EndPoint Control	0x00017abb	Info	Endpoint Control Registration Status changed to [status] with FGT [serial]	
EndPoint Control	0x00017abc	Info	Endpoint Quarantine Status changed to [status]	Endpoint Quarantine Status Changed
Update	0x00017a2a	Info	Customer initiated a software update request.	Logged when a user presses the gui's update button.
Update	0x00017a37	Info	Checking for updates.	Checking for updates.
Update	0x00017a2c	Info	Update allowed only if you have a valid license	Update allowed only if you have a valid license

Client Feature	ID	Level	Format	Description
Update	0x00017a38	Info	Software update started.	Software update started.
Update	0x00017a2d	Info	Software updates are disabled.	Software updates from FortiGuard have been disabled.
Update	0x00017a2e	Info	Software updates from FortiGuard have been disabled because this client is managed.	Software updates from FortiGuard have been disabled.
Update	0x00017a2f	Info	Software updates require administrative privileges.	The user does not have sufficient privileges to perform software updates.
Update	0x00017a30	Info	Software update successful.	Software update successful.
Update	0x00017a31	Info	Software update failed.	Software update failed.
Update	0x00017a32	Info	Unable to perform software update. Registry does not contain image id to download.	The image id that is expected to be in the registry is missing.
Update	0x00017a33	Info	Update <module description> successful	
Update	0x0001798a	Info	Update success	Update was successful.
Update	0x00017a34	Error	Unable to load AV engine	Failed to load the av engine
Update	0x00017a35	Error	Error patching AV signature.	Error patching AV signature.
Update	0x00017a36	Error	Unable to load FASLE engine	Unable to load FASLE engine
Update	0x00017a39	Info	Update successful	
Scheduler	0x00017a20	Info	Forcefully kill a child process after grace period expires	A scheduler owned child process failed to stop when instructed to do so

Client Feature	ID	Level	Format	Description
Scheduler	0x00017a21	Error	The scheduler cannot start the scheduled task because the task's license is expired.	The scheduler cannot start the scheduled task because the task's license is expired.
Scheduler	0x00017a68	Info	FortiClient is starting up	FortiClient is starting up
Scheduler	0x00017a69	Info	%s is shutting down	FortiClient is shutting down
FortiProxy	0x00017a49	Info	Fortiproxy is enabled	Fortiproxy is enabled
FortiProxy	0x00017a48	Warning	Fortiproxy is disabled	Fortiproxy is disabled
FortiShield	0x00017a53	Info	FortiShield is enabled	FortiShield is enabled
FortiShield	0x00017a52	Warning	FortiShield is disabled	FortiShield is disabled
FortiShield	0x00017a54	Info	The console was locked	The console password was locked.
FortiShield	0x00017a55	Warning	The console was unlocked	The console password was unlocked.
FortiShield	0x00017a56	Warning	The console password was removed	The console password was removed.
FortiShield	0x00017a57	Warning	FortiShield blocked application: [application path] from modifying: [file or registry path]	FortiShield has prevented an application from modifying a file or registry setting protected by FortiClient.
Application Database	0x0000d001	Error	<context> <file reference> db error - creating new database.	A critical error occurred. The application database will not work. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d003	Error	<context> <file reference> db error - BIND command.	A critical error occurred. The application database will not work. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d004	Error	<context> <file reference> db error - opening database.	A critical error occurred. The application database is not present. An attempt to automatically regenerate it will occur. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d005	Error	<context> <file reference> db error - preparing sql statement.	The sql statement used is invalid. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d006	Error	<context> <file reference> db error - unable to find fingerprint.	The fingerprint does not exist in the database. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d007	Error	<context> <file reference> db error - invalid md5.	The parameter supplied is not an MD5. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d008	Error	<context> <file reference> db error - row not found.	The requested row does not exist. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00a	Error	<context> <file reference> Can't open file.	The file cannot be opened. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00b	Error	<context> <file reference> Unable to extract vendor id.	The files is not digitally signed
Application Database	0x0000d00e	Error	<context> <file reference> Can't access file because of sharing violation.	Can't access file because of sharing violation. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00f	Error	<context> <file reference> Can't open driver.	Can't open the apd driver. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d010	Error	<context> <file reference> Can't start driver.	Can't start the apd driver. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d011	Error	<context> <file reference> Driver io error.	APD driver io error. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d016	Error	<context> <file reference> Server-side pipe error.	A communication error occurred. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d017	Error	<context> <file reference> Pipe server initialization error.	A communication initialization error occurred. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d018	Error	<context> <file reference> Pipe server creation error.	A communication initialization error occurred. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d019	Error	<context> <file reference> Unable to bypass fortishield.	Failed to bypass self-protection. The daemon might not function normally after this. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01a	Error	<context> <file reference> Invalid arguments.	Invalid command line options supplied. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d01c	Error	<context> <file reference> Unable to allocate memory for vendor id cache.	Low memory. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01d	Error	<context> <file reference> Vendor id cache not initialized.	This is probably temporary. An attempt will be made later to read/write to the cache. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01e	Error	<context> <file reference> Unable to open vendor id cache shared memory.	Application detection will not be functioning normally. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01f	Error	<context> <file reference> Unable to open mutex to access vendor id shared memory.	Application detection will not be functioning normally. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Config Import/Export	0x00017a5c	Info	A configuration file is exported to [location]	Logged when someone exports a config file.
Config Import/Export	0x00017a5d	Info	A configuration file is imported from [location]	Logged when someone imports a config file.
Config Import/Export	0x00017a72	Info	Policy '[name]' was received and applied	Logged when push configuration is received.
Single Sign-On Mobility Agent	0x00017ad4	Info	Single Sign-On event	Single Sign-On event.

Client Feature	ID	Level	Format	Description
Single Sign-On Mobility Agent	0x00017ad5	Info	Single Sign-On Mobility Agent was enabled	Logged when someone enables Single Sign-On Mobility Agent.
Single Sign-On Mobility Agent	0x00017ad6	Warning	Single Sign-On Mobility Agent was disabled	Logged when someone disables Single Sign-On Mobility Agent.
Single Sign-On Mobility Agent	0x00017ad7	Info	Single Sign-On Mobility Agent is starting…	
Single Sign-On Mobility Agent	0x00017ad8	Info	Single Sign-On Mobility Agent is stopping…	
UI	0x00017a66	Warning	Logs were cleared	Logged when logs are cleared.
UI	0x00017a67	Info	Alerts were cleared	Logged when alerts are cleared by a user.

Appendix E - Vulnerability Patches

FortiClient checks many applications for vulnerabilities. FortiClient can automatically patch vulnerabilities from some applications, but not all applications. For some applications, the user must manually patch vulnerabilities.

For the latest list of supported software, see the FortiGuard Center (FortiGuard.com) .

Automatic vulnerability patching

FortiClient automatically patches vulnerabilities for the following software:

- 7-ZIP
- Adobe Flash Player Active X plug-in for Internet Explorer
- Adobe Flash Player NPAPI plug-in for Firefox
- Adobe Reader
- Adobe Reader DC
- Adobe Acrobat
- Adobe Acrobat DC
- Adobe AIR
- Apple iTunes
- Microsoft Security Bulletins
- Mozilla Firefox
- Mozilla Firefox ESR
- Mozilla Thunderbird
- Oracle Java JRE
- PostgreSQL (version 9.1 and later)
- VideoLan VLC Media Player
- VMware player
- VMware Workstation Player
- Wireshark

Manual vulnerability patching

FortiClient automatically checks the following software for vulnerabilities, but cannot automatically patch vulnerabilities. The user must manually install updates to the following software to patch vulnerabilities:

- Adobe AIR SDK
- Adobe Acrobat X
- Adobe Acrobat Reader X
- Adobe Shockwave Player
- Apple QuickTime

- Apple Safari
- Jave JDK
- Google Chrome
- Google Picasa
- Oracle MySQL server
- PHP
- PostgreSQL (earlier than version 9.1)

FORTINET®

High Performance Network Security

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.